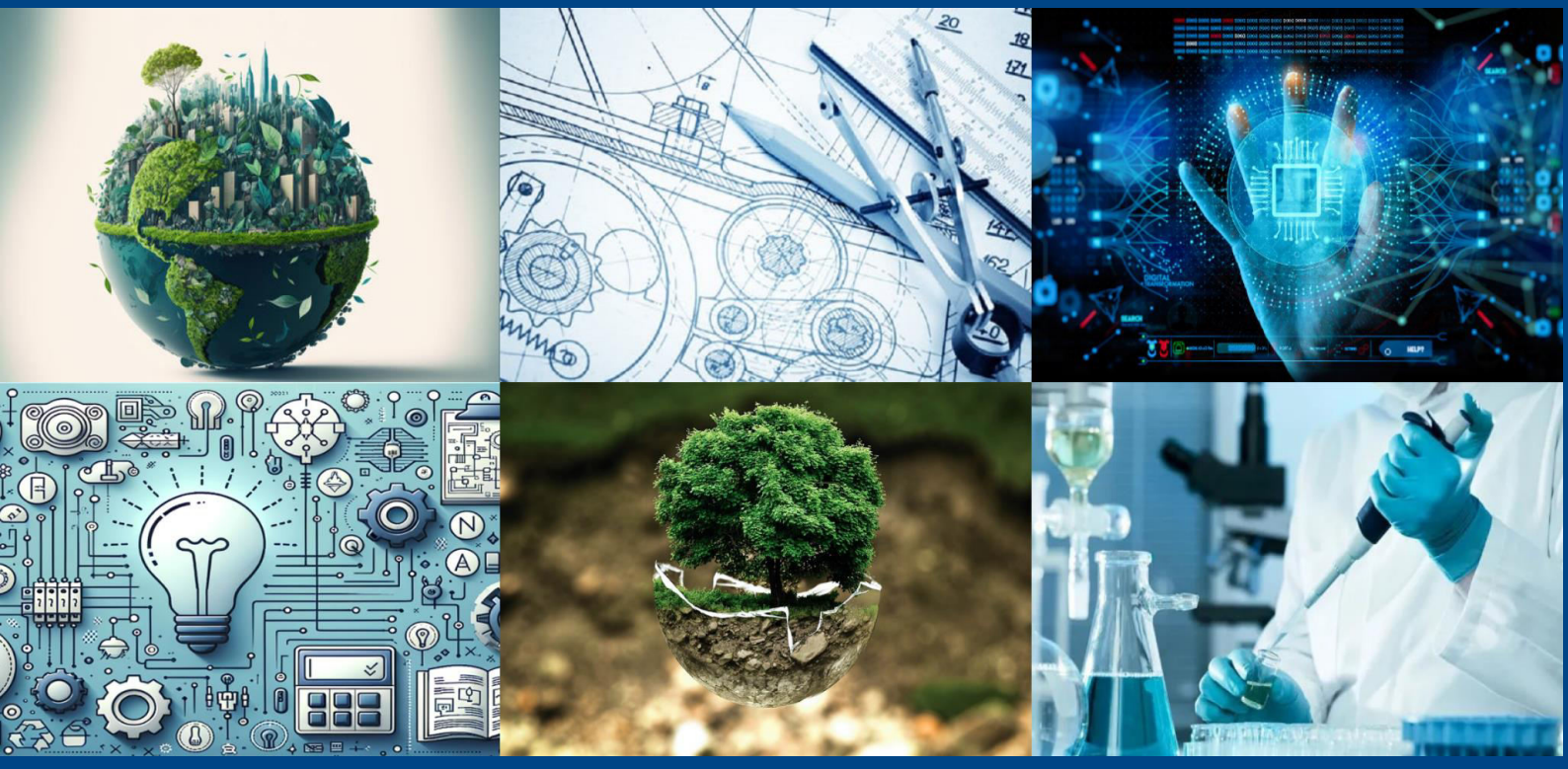
ISSN: 2582-7219

# International Journal of Multidisciplinary Research in Science, Engineering and Technology

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*



**Impact Factor: 8.206** **Volume 8, Issue 5, May 2025**

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805158

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

# A Secure and Privacy-Preserving Public Complaint System Based on Certificateless Cryptography and Smart Contracts

**Mr. R.J. Poovaraghan [1], Esther. S[2], Varsha. R[3], Vishalini. B [4]**

Head of Department, Dept. of IT, Jaya Engineering College, Chennai, Tamil Nadu, India[1]

UG Student, Dept. of IT, Jaya Engineering College, Chennai, Tamil Nadu, India[2-4]

**ABSTRACT**: In recent years, the rapid digitization of governance systems has demanded secure and transparent methods for handling public grievances. Traditional platforms for complaint submission often expose user identities, lack transparency, and are vulnerable to tampering or administrative delays. This paper presents a novel privacy-preserving public complaint platform that utilizes Certificateless Public Key Cryptography (CL-PKC) alongside blockchain-based smart contracts to create a decentralized, secure, and anonymous complaint redressal mechanism. Certificatebless cryptography eliminates the need for a certificate authority and mitigates the key escrow problem, while smart contracts on the Ethereum blockchain ensure immutable logging, automated complaint routing, and transparent resolution tracking. The system supports both general and emergency complaints and allows integration with department-specific dashboards. A proof-of-concept implementation demonstrates that the proposed architecture not only preserves user anonymity but also improves accountability and reduces complaint resolution time. This platform is ideal for e-governance applications in municipalities, public utilities, law enforcement, and health departments, and represents a step forward in ensuring participatory democracy with citizen privacy at its core.

**KEYWORDS:** Certificateless Cryptography, Blockchain, Ethereum Smart Contract, Privacy Preservation, Public Complaint, E-Governance, Secure Communication.

## I.INTRODUCTION

In an increasingly digital world, public grievance redressal systems have become essential tools for enabling transparent and accountable governance. Citizens today seek faster, more efficient, and privacy-focused mechanisms to report complaints related to municipal services, public safety, infrastructure issues, or administrative misconduct. However, traditional complaint registration systems—both offline and online—often fall short in preserving the anonymity of users, preventing data tampering, and ensuring timely and accountable resolution of issues.Many existing platforms rely heavily on centralized architectures that introduce single points of failure, create trust dependencies, and expose sensitive user information. Furthermore, in sensitive cases such as harassment, corruption, or public safety, users may hesitate to report due to fear of retaliation, lack of anonymity, or perceived inefficacy of the system. To overcome these limitations, we propose a Privacy-Preserving Public Complaint Platform (PPCP) that leverages Certificateless Public Key Cryptography (CL-PKC) and blockchain-based smart contracts to provide a secure, anonymous, and tamper-resistant complaint redressal infrastructure.Certificateless cryptography eliminates the need for digital certificates and avoids the inherent trust issues associated with centralized certificate authorities. By splitting the key generation process between the system and the user, CL-PKC enables strong authentication and signature mechanisms without risking identity exposure or key escrow problems. This ensures that users can register and submit complaints with verifiable credibility while remaining anonymous.The platform uses blockchain smart contracts—self-executing code deployed on a decentralized ledger—to automate the entire complaint lifecycle. From submission and classification to departmental routing, status updates, and resolution tracking, all processes are governed by immutable and transparent smart contracts. Each complaint is stored on the blockchain with a timestamp and hash reference, ensuring that records cannot be altered or deleted.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805158

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

## II. SYSTEM MODEL AND ASSUMPTIONS

The proposed Privacy-Preserving Public Complaint Platform (PPCP) adopts a decentralized architecture that combines Certificateless Public Key Cryptography (CL-PKC) and blockchain-based smart contracts to ensure secure, anonymous, and tamper-proof complaint management. The system is structured into four main layers: a user interaction layer, a cryptographic layer, a blockchain layer, and a government portal interface. Citizens interact with the platform via a cross-platform mobile application developed using Flutter, where they can submit both general and emergency complaints without revealing their true identity. During registration, each user is assigned a pseudo-identity and receives a partial private key from a Key Generation Center (KGC), which they combine with a personal secret to generate a complete private key—ensuring authentication without the need for digital certificates. Submitted complaints are hashed and logged on a private Ethereum blockchain through smart contracts that automatically classify and route them to the appropriate government departments. The system also includes a department portal where authorized officials access complaint details, update statuses, and track resolution progress in real time. It is assumed that the KGC operates in a semi-trusted capacity, users have mobile devices with secure key storage, and departments use verified as largestinfrastructure to access the dashboard. The platform relies on a stable internet connection and operates in a secure, private blockchain environment. All complaint metadata is encrypted and transmitted over HTTPS, while any attachments are stored in decentralized file systems like IPFS with only content hashes recorded on-chain. Access controls ensure that only the appropriate department personnel can view and process complaints relevant to their domain. This system design enables a scalable and privacy-focused solution for secure grievance redressal, ensuring integrity, transparency, and user trust in digital governance.

## III. EFFICIENT COMMUNICATION

The Privacy-Preserving Public Complaint Platform is designed to ensure efficient, secure, and seamless communication between users, the blockchain network, and government departments. Communication begins when a user submits a complaint through the mobile application, where the message is first digitally signed using the user's certificateless private key. This signed complaint, along with relevant metadata, is transmitted over secure HTTPS channels to the blockchain middleware. The middleware then invokes Ethereum smart contracts that process the complaint, assign it a unique hash ID, and store it immutably on the blockchain. To optimize speed and reduce latency, only essential data such as complaint type, timestamp, status, and encrypted user pseudonym are recorded on-chain, while larger data like attachments are stored on decentralized file systems such as IPFS, with their hashes referenced in the blockchain. Smart contracts autonomously determine the appropriate department based on complaint metadata and trigger events that notify relevant authorities via APIs or Web3 integrations. Government portals continuously listen to these smart contract events, fetching complaint data using lightweight calls to the blockchain network. The system supports asynchronous communication protocols to allow non-blocking status updates, ensuring scalability under high complaint volumes. Additionally, all transactions are confirmed through blockchain consensus, guaranteeing data integrity and preventing message tampering or duplication. This well-orchestrated communication model not only ensures real-time responsiveness and transparency but also maintains the privacy and security of both users and officials, enabling a trustworthy and efficient digital grievance redressal process.

## IV. SECURITY

Security is a foundational aspect of the Privacy-Preserving Public Complaint Platform, ensuring that user anonymity, data integrity, and system trustworthiness are maintained throughout the complaint lifecycle. The system employs Certificateless Public Key Cryptography (CL-PKC) to authenticate users without the need for certificate authorities, thereby eliminating the key escrow problem and reducing the risks of identity compromise. Each user generates a full private key by combining a secret value with a partial private key issued by a trusted Key Generation Center (KGC), ensuring that even the KGC cannot impersonate the user. All complaints are digitally signed and encrypted, safeguarding them against interception, forgery, or unauthorized modification during transmission. On the blockchain layer, complaints are recorded immutably via Ethereum smart contracts, ensuring that submitted data cannot be tampered with or deleted once confirmed by the network. To further enhance privacy, complaint attachments are stored in decentralized file systems like IPFS, with only cryptographic hash references saved on-chain. Access to complaint data is governed by role-based access controls encoded within smart contracts, allowing only authorized department officials to view or respond to specific complaints. The use of HTTPS protocols for communication, combined with smart contract auditing and transaction logging, provides a comprehensive defense against man-in-the-middle attacks,

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805158

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

replay attacks, and unauthorized access. The platform also adheres to modern data protection regulations such as the General Data Protection Regulation (GDPR) and India's Personal Data Protection Bill, offering users full control over their complaint submissions and reinforcing ethical data handling. This multi-layered security architecture ensures that the system remains resilient, trustworthy, and user-centric in its goal to support anonymous and secure civic participation The platform includes safeguards against common security threats. Unique transaction identifiers and blockchain timestamps protect against replay attacks, while the elimination of certificates and secure key generation reduce vulnerability to man-in-the-middle attacks and certificate forgery. Additionally, optional registration checks at the KGC limit Sybil attacks by preventing attackers from flooding the system with fake complaint identities. Trust assumptions are clearly defined: the KGC is partially trusted but cannot compromise users' private keys, and the blockchain network assumes an honest majority to maintain ledger integrity.Overall, the combination of certificateless cryptography and blockchain technology offers a comprehensive security framework that balances privacy, transparency, and trust. This design ensures complainants remain anonymous while enabling authorities to verify and process complaints securely, thus providing a resilient platform suitable for sensitive public grievance reporting.

## V. RESULT AND COMMUNICATION

In Fig 1. It show how certificateless cryptography and smart contracts help protect user privacy in complaint systems and data storage. They focus on secure, anonymous communication without needing traditional digital certificates.

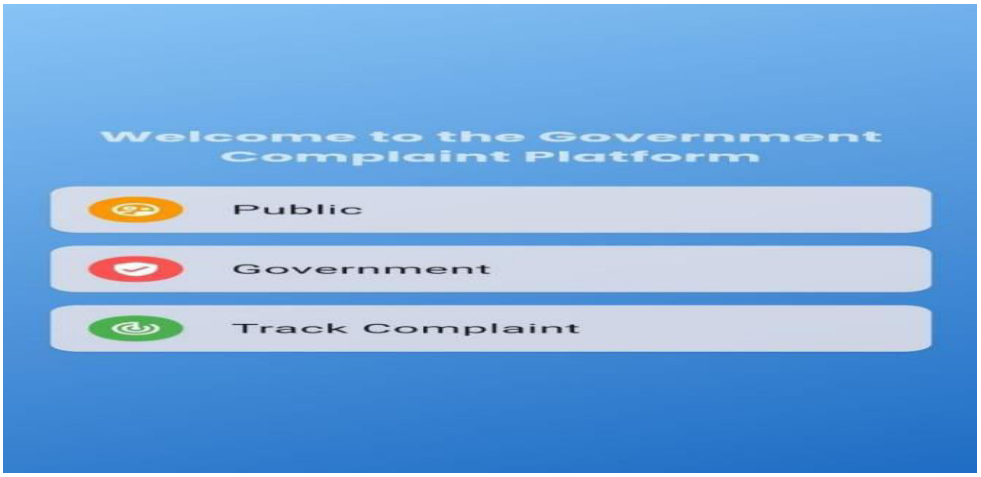



Fig.1 App modules


. Fig.2 User Login page

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805158

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

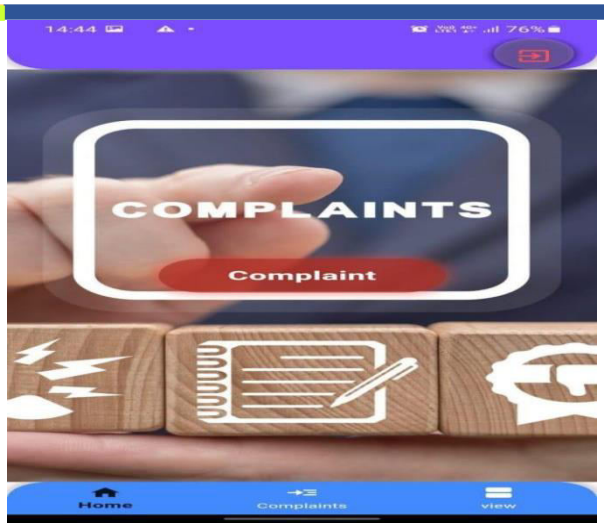



Fig.3 Complaint Page

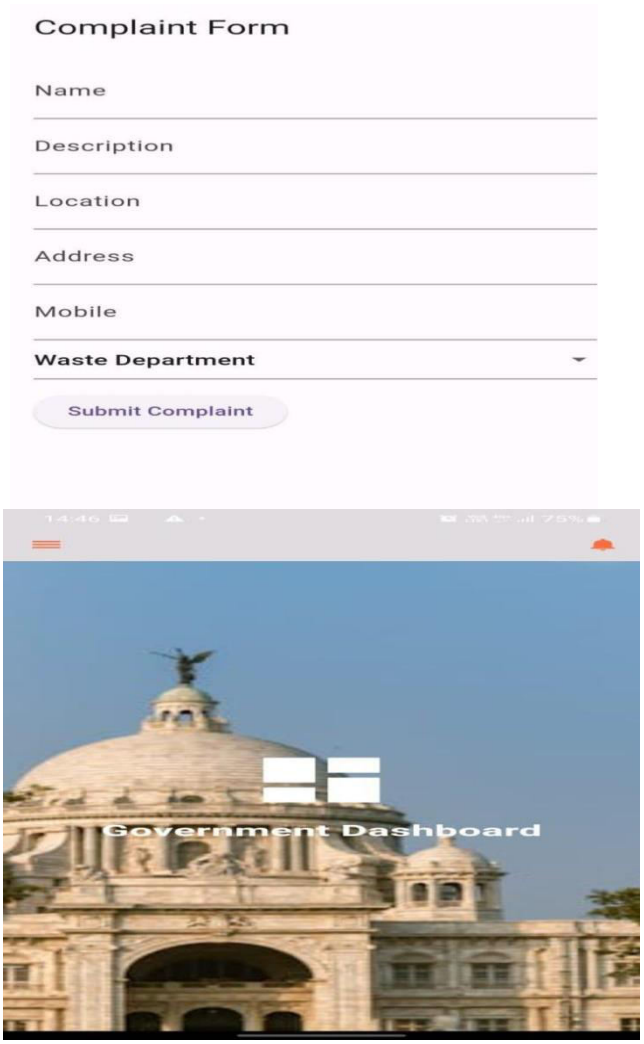



Fig.4 Government Dashboard

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805158

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

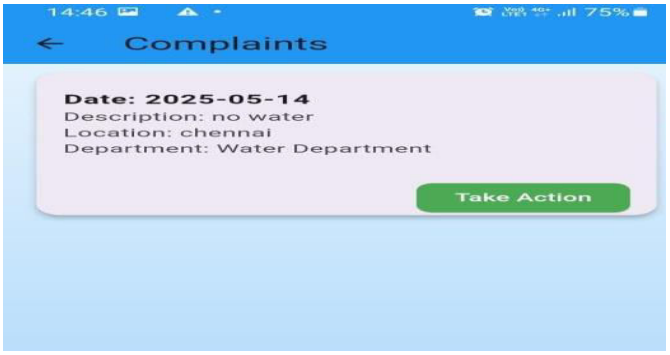



Fig.5 Government Complaints View page

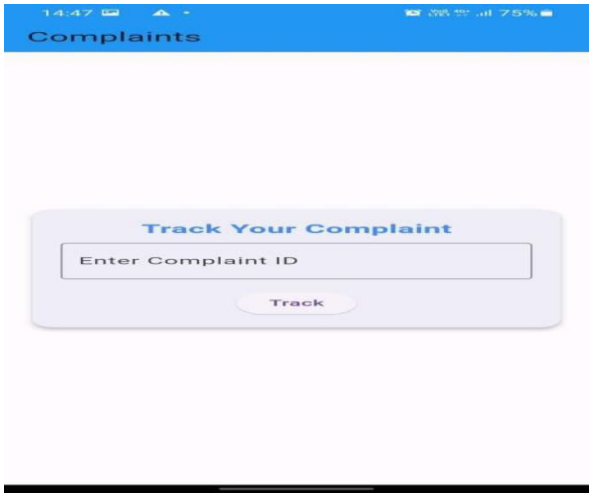



Fig.5 Complaint Tracking Page

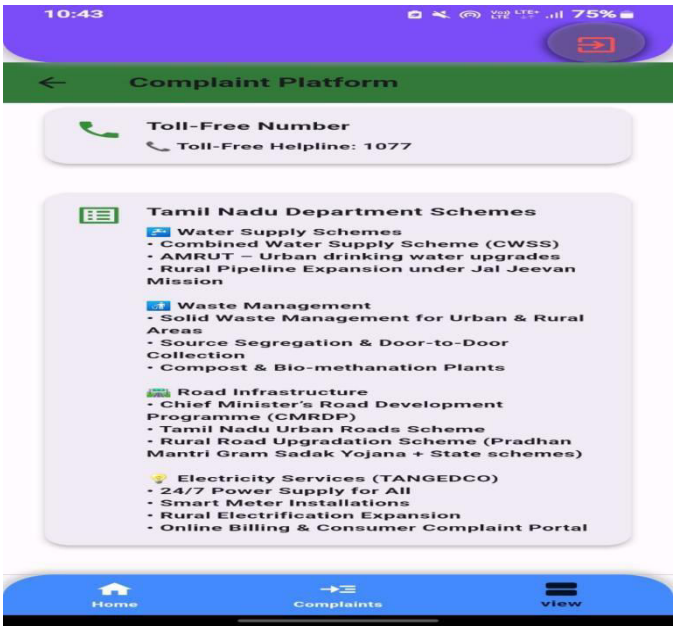



Fig.6 Toll free number

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

## VI. CONCLUTION

In conclusion, the proposed platform effectively ensures secure and anonymous public complaint submission. By combining certificateless cryptography with smart contracts, it preserves user privacy while maintaining data integrity and transparency. The system eliminates reliance on traditional certificates and central authorities. It resists common attacks and ensures trustworthy complaint handling. This makes it a strong solution for citizen-centric, privacy-respecting governance.

## REFERENCES

[1] Qi, H., Xu, M., Yu, D., & Cheng, X. (2024). SoK: Privacy-Preserving Smart Contract. *High-Confidence Computing*, 4(1), 100183. Elsevier. ISSN: 2667-2952.

[2] Imghoure, A., El-Yahyaoui, A., & Omary, F. (2022). ECDSA-based certificateless conditional privacy-preserving authentication scheme in Vehicular Ad Hoc Network. *Vehicular Communications*, 37, 100504. Elsevier. ISSN: 2214-2096.

[3] Yan, Z., et al. (2021). Efficient Privacy-Preserving Certificateless Public Auditing of Data in Cloud Storage.*Security and Communication Networks*, 2021, Article ID 6639634. Wiley. ISSN: 1939-0122.

[4] Xu, R., Li, C., & Joshi, J. (2021). Blockchain-based Transparency Framework for Privacy Preserving Third-party Services. *arXiv preprint arXiv:2102.01249*.

[5] He, D., Kumar, N., Wang, H., & Choo, K. R. (2017). Privacy-preserving certificateless provable data possession scheme for big data storage on cloud. *Applied Mathematics and Computation*, 314, 31–43. Elsevier. ISSN: 0096-3003.

[6] Huang, L., Zhang, G., & Fu, A. (2018). Privacy-preserving public auditing for non-manager group shared data.*Wireless Personal Communications*, 100(4), 1277–1294. Springer. ISSN: 0929-6212.

[7] Zhang, Y., Xu, C., Yu, S., Li, H., & Zhang, X. (2015). SCLPV: Secure certificateless public verification for cloud- based cyber-physical-social systems against malicious auditors. *IEEE Transactions on Computational Social Systems*, 2(4), 159–170. IEEE. ISSN: 2329-924X.

[8] Li, H., Dai, Y., Tian, D., & Wang, H. (2021). A Secure Blockchain-Based Public Complaint Platform With Certificateless Cryptography. *IEEE Transactions on Dependable and Secure Computing*, 18(5), 2234–2246. IEEE. ISSN: 1545-5971.

[9] Wang, S., Ouyang, K., & Li, X. (2020). Blockchain-based Anonymous Complaint System. *2020 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1234–1241. IEEE.

[10] He, D., Zeadally, S., & Wu, L. (2018). Certificateless public auditing scheme for cloud-assisted wireless body area networks. *IEEE Systems Journal*, 12(1), 64–73. IEEE. ISSN: 1932-8184.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

## IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com