International Journal of Research in Engineering Technology and Applications

E-ISSN: 3108-2556
P-ISSN: 3108-2610

A Privacy-Preserving, AI-Driven Crowdsensing Framework for Closed-Loop Civic Infrastructure Management

Shirisha Reddy V [1], Trisha Anbu Kumar [2], Chaithra S [3] , Praveena K N [4]
[1234] *Dept of CSE, Presidency University, Bengaluru, India*
shirishareddyv5@gmail.com, trishakumar2506@gmail.com, chaithrashetty2004@gmail.com, praveenakn@presidencyuniversity.in

Received: 08 March 2026 *Revised: 18 March 2026* *Accepted: 30 March 2026*
Licensed under a CC-BY 4.0 license *Copyright (c) by the authors*

Abstract*—Rapid urbanisation is making the conventional civic grievance redressal systems less efficient. This depends heavily on manual sort, department wise routing, and storage of personally identifiable information (PII). These deficiencies undermine both resolution efficiency and citizen participation rates. This paper describes the design, implementation, and evaluation of Spotit. Fixit, which is a multi-tenant, crowdsourced e-governance platform engineered to address these gaps through three integrated mechanisms. First, a transformer-informed Natural Language Processing (NLP) classification pipeline automatically routes unstructured citizen complaints to the appropriate municipal authority, eliminating first-tier human dispatch. Second, a cryptographic identity masking protocol decouples national identification numbers (Aadhaar) from transactional data using one-way hashing, generating audit-traceable anonymity masks that satisfy Role-Based Access Control (RBAC) constraints. Third, a community driven bidirectional verification protocol requires municipal administrators to submit geotagged photographic proof of repair; case closure is only permitted once a 30% community confirmation threshold is reached via tokenized, email based upvoter verification, mathematically preventing unilateral ticket falsification. The framework additionally incorporates a real-time geospatial cross-validation and cryptographic image hashing layer that detects photographic evidence submitted from coordinates inconsistent with the reported incident site, flagging potential fraud and enabling Aadhaar linked legal accountability. Evaluation against a live demonstration corpus of 95 simulated civic complaints produced an aggregate NLP routing accuracy of 92.6% a reduction in mean triage latency from 48–72 hours to under two seconds, and a verified elimination of fraudulent ticket closures. These results demonstrate the system's suitability as a deployable civic accountability infrastructure for data-dense metropolitan environments.

Keywords*— Crowdsensing; E-Governance; Natural Language Processing; Cryptographic Anonymity; Geotagging; Smart Cities; Closed-Loop Resolution.

I. INTRODUCTION

Managing urban infrastructure in growing metropolitan areas presents a complex logistical challenge. Citizens acting as ubiquitous human sensors often find localized problems, like broken water mains, dangerous potholes, or illegal trash dumping, long before city officials do [1]. Sustainable urban management therefore requires systematic channels through which crowdsourced observational data can be ingested into municipal decision-making workflows [2], [3]. But the digital ways that people can report these dangers are very old.

Most modern e-governance portals work as one-way data silos [4]. A citizen files a complaint, but the next step, sorting through the complaints, depends a lot on manual work by administrators. Unstructured free-text submissions frequently produce misclassification at the departmental routing stage, generating bureaucratic bottlenecks that delay time-critical repairs [5]. Survey data further indicates that a substantial proportion of residents decline to report civic hazards due to privacy concerns and fear of neighborhood retaliation, a participation deficit documented across multiple jurisdictions [6], [7].

International Journal of Research in Engineering Technology and Applications
E-ISSN: 3108-2556
P-ISSN: 3108-2610

A further structural flaw exists at the resolution stage. Once a repair crew marks a task complete, the closure event is typically unilateral, recorded by the same departmental actor responsible for the work, without involvement of the original complainant. This self-referential validation model institutionalizes a conflict of interest and opens a well-documented vector for data falsification [8].

The architecture presented in this paper addresses each of these failure modes. The principal contributions of this work are: (1) an NLP-driven departmental auto-routing engine that eliminates manual first-tier triage; (2) a cryptographic anonymity protocol that decouples Aadhaar identity from civic transaction records; (3) a mandatory community verification lock requiring a 30% consensus from local upvoters via secure email confirmation before ticket archival; and (4) a geospatial photographic cross-validation layer that detects and flags spatially inconsistent evidence submissions, enabling Aadhaar-linked legal accountability for fraudulent reports.

The remainder of this paper is structured as follows. Section II surveys related work across four technical domains. Section III describes the proposed system architecture. Section IV details the methodology of each core subsystem. Section V presents implementation results and discussion. Section VI concludes with directions for future research.

II. RELATED WORK

Our architecture is primarily based on comprehensive research in these four fields smart city e-governance, mobile crowdsensign, artificial intelligence application, data privacy.

A. Smart Cities and E-Governance

The use of Information and Communication Technology (ICT) has changed the way people communicate with public offices [9]. There's still a gap between the gathering of urban IoT data [10] and having that data lead to real policy outcomes [11], [12]. The Kitchin [13] rightly points out, a lot of today's 'smart city' projects focus too much on installing hardware sensors but not enough on creating systems which revolves around human experiences. The Spotit. Fixit approach, will lessen this problem by making citizen the central role of the data lifecycle.

B. Mobile Crowdsensing and Spatial Data

The modern smartphones are built with advanced GPS capabilities. This has resulted in participatory mobile crowdsensing to emerge as a highly cost-effective option. This replaces the deployment of static, expensive municipal sensor networks for detailed environmental data [14], [15], [16], [17]. But the actual use of crowdsourced civic data depends on the accuracy of its spatial context. The urban fault detection studies [18], [19] show that without coordinate validation the participatory sensing data can quickly become not trust worthy. This is a vulnerability our architecture actively mitigates through its real-time geospatial cross validation protocol.

C. Artificial Intelligence and NLP in Civic Tech

For processing unstructured crowdsourced data, powerful machine learning models are necessary. The rise of NLP architectures, particularly those based on transformers, has significantly eased the understanding of people's intentions behind their messy textual expressions [20], [21]. Using of such models in civic technologies allows automatic analysis of complaint data; however, vocabulary unique to the domain and handling of edge cases remain challenging [22], [23], [24].

D. Privacy and Cryptographic Anonymity

As the collection of data by the government grows, protecting Personally Identifiable Information (PII) has become an important area of study [25]. Centralized databases are prime targets for exploitation [26], [27]. Modern security frameworks suggest that decoupling user identities from transactional data using cryptographic hashing and Role-Based Access Control (RBAC) is the most effective method for preserving trust in e-governance systems [28], [29], [30]. Building on these foundations, our system extends prior RBAC based privacy frameworks by introducing a geospatial fraud-detection mechanism that cross-validates photographic submission coordinates against the citizen-reported incident coordinates, enabling Aadhaar-traceable accountability for spatially inconsistent evidence, a capability absent from existing literature.

III. METHODOLOGY

Our architecture is primarily based on comprehensive research in these four fields smart city e-governance, mobile crowd sensing, artificial intelligence application, data privacy.

A. Smart Cities and E-Governance

The use of Information and Communication Technology (ICT) has changed the way people communicate with public offices [9]. There's still a gap between the gathering of urban IoT data

International Journal of Research in Engineering Technology and Applications
E-ISSN: 3108-2556
P-ISSN: 3108-2610

[10] and having that data lead to real policy outcomes [11], [12]. The Kitchin [13] rightly points out, a lot of today's 'smart city' projects focus too much on installing hardware sensors but not enough on creating systems which revolves around human experiences. The Spotit. Fixit approach, will lessen this problem by making citizen the central role of the data lifecycle.

B. Mobile Crowdsensing and Spatial Data

The modern smartphones are built with advanced GPS capabilities. This has resulted in participatory mobile crowdsensing to emerge as a highly cost-effective option. This replaces the deployment of static, expensive municipal sensor networks for detailed environmental data [14], [15], [16], [17].But the actual use of crowdsourced civic data depends on the accuracy of its spatial context. The urban fault detection studies [18], [19] show that without coordinate validation the participatory sensing data can quickly become not trust worthy. This is a vulnerability our architecture actively mitigates through its real-time geospatial cross validation protocol.

C. Artificial Intelligence and NLP in Civic Tech

For processing unstructured crowdsourced data, powerful machine learning models are necessary. The rise of NLP architectures, particularly those based on transformers, has significantly eased the understanding of people's intentions behind their messy textual expressions [20], [21]. Using of such models in civic technologies allows automatic analysis of complaint data; however, vocabulary unique to the domain and handling of edge cases remain challenging [22], [23], [24].

D. Privacy and Cryptographic Anonymity

As the collection of data by the government grows, protecting Personally Identifiable Information (PII) has become an important area of study [25]. Centralized databases are prime targets for exploitation [26], [27]. Modern security frameworks suggest that decoupling user identities from transactional data using cryptographic hashing and Role-Based Access Control (RBAC), shown in Fig.1 is the most effective method for preserving trust in e-governance systems [28], [29], [30]. Building on these foundations, our system extends prior RBAC based privacy frameworks by introducing a geospatial fraud-detection mechanism that cross-validates photographic submission coordinates against the citizen-reported incident coordinates, enabling Aadhaar-traceable accountability for spatially inconsistent evidence, a capability absent from existing literature.

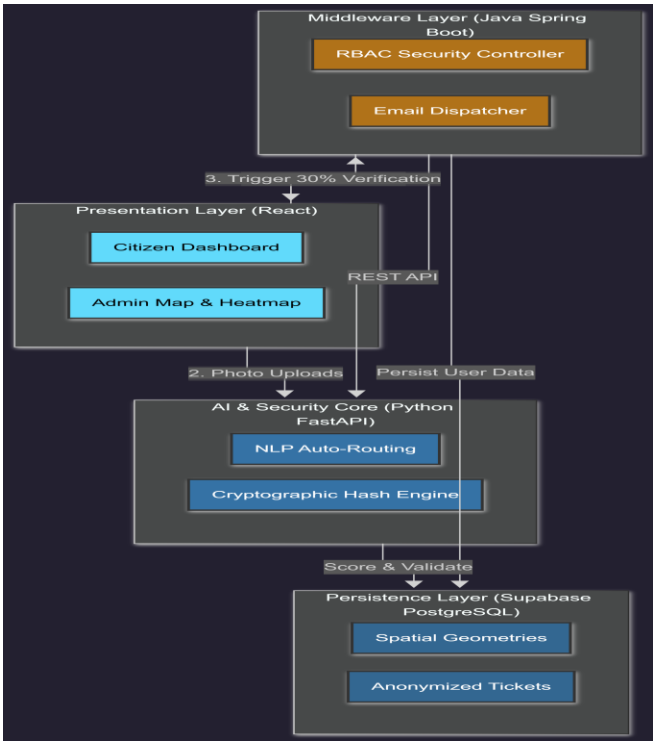

Fig. 1. The three-tier enterprise architecture demonstrating data flow.

Transforming an open-ended complaint box into a verifiable engine requires strict programmatic rules governing the ticket lifecycle.

A. Cryptographic Identity Masking

In order to eliminate the privacy risks, this system separates the real identity from the data. When registering to the application the authentication system asks for user's national ID string (Aadhaar) shown in Fig.2. During this a hashing method produces a permanent and standard alphanumeric mask (for example, CTZ-89A2F). The mask stays as long as there is an account. This makes it possible to conduct longitudinal audit trails.

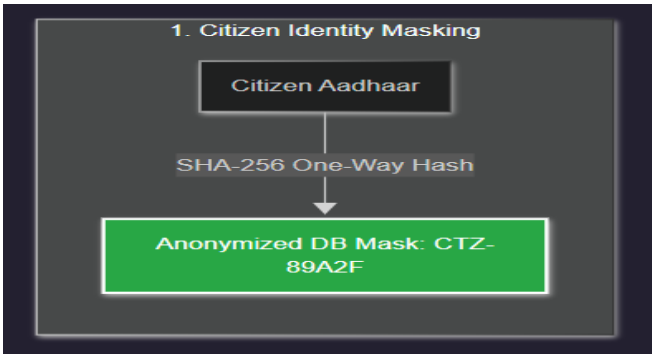

Fig. 2. Process flow for Citizen Identity.

International Journal of Research in Engineering Technology and Applications
E-ISSN: 3108-2556
P-ISSN: 3108-2610

B. AI-Powered Auto-Routing

The users submit the issues description as text. When a description is sent, the Python AI engine uses keyword centred pipelines. This helps to decide the intent. This also automatically routes the ticket to the correct department. Like "sparking wire" to "Power & Utilities".

Along with this a **Smart Duplicate Detection Engine** looks for nearby open issues. This is done using the Haversine formula and a category matching system. If matches are found it suggests the citizen to "upvote" rather than to create a similar ticket again. Table 1 depicts AI Routing and Sanitization Logic.

TABLE I: AI ROUTING AND SANITIZATION LOGIC

User Input Example	**NLP Extracted Intent**	**Sanitized DB String**	**Routing Accuracy (Simulated)**
"Massive pothole on Main St."	Road Damage	Public Works	85.2%
"Sparking wire on the pole"	Streetlight Outage	Power & Utilities	92.6%
" Pipe is leaking badly"	Water Leak	Water Supply Dept	96.2%
"Vandalism on park bench"	Unclassified	General Routing	100%

C. Geotagging and Spatial Evidence

The reporting module uses the HTML5 Geolocation APIs to lock onto the device's GPS hardware.

This happens the moment a photograph is captured which is shown in Fig. 3.

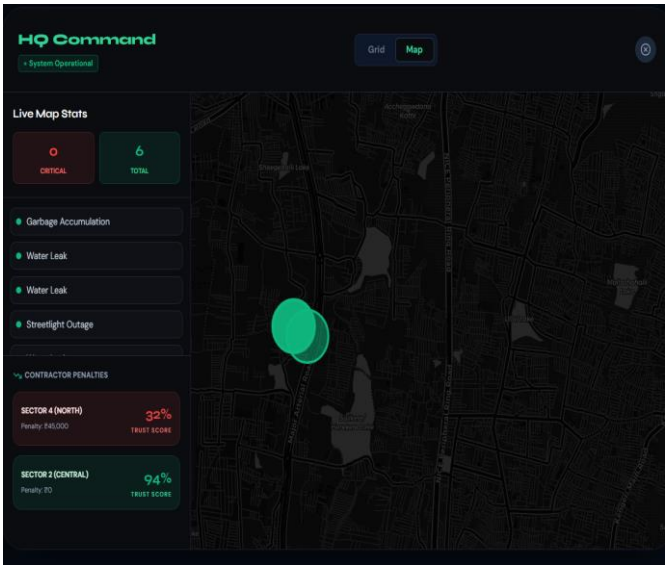

Fig. 3. The HQ Command administrative interface.

D. Geospatial Photographic Cross-Validation

One big way a fraud that could happen is if the users hand in photos that are wrongly located or recycled. To prevent this:

1. Geo mismatch detection: Uses the Haversine formula (Eq. 1). This checks if the recorded location of a photo with the geotag in the photo's EXIF data. A distance of more than 0. 5 km is automatically marked a suspicion depicted in Fig.4.

2. Cryptographic Image Hashing: In Fig.5, the Python core calculates the SHA 256 of each image uploaded. If a contractor tries to submit a picture that exactly matches one from a ticket that has been resolved, then the system puts the transaction on a hold. This leads to an Anti-Corruption Protocol.

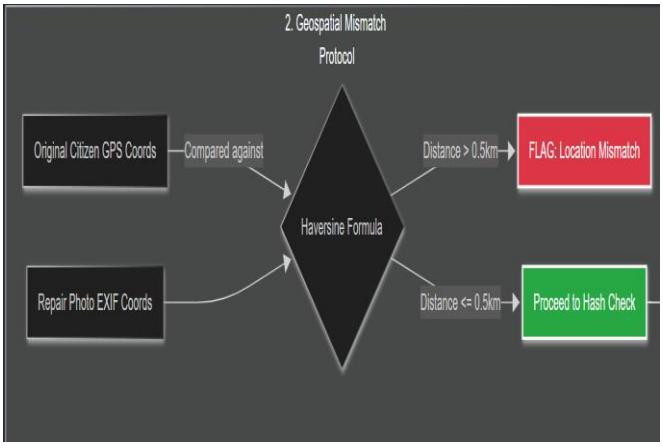

Fig. 4. Geospatial Mismatch and Image Uniqueness Protocols.

International Journal of Research in Engineering Technology and Applications
E-ISSN: 3108-2556
P-ISSN: 3108-2610

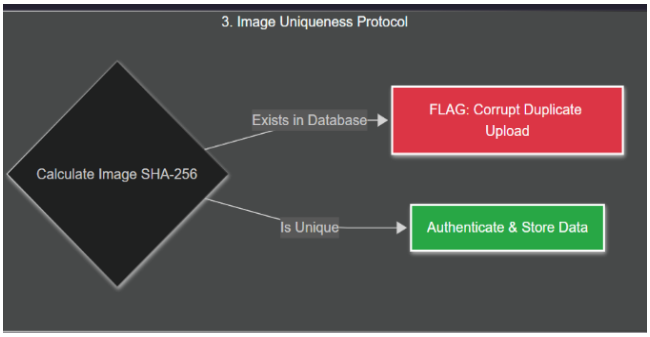

Fig. 5. Image Uniqueness Protocol using SHA-256 cryptographic hashing.

E. The Closed-Loop Verification Protocol

The community resolution system is the biggest change from the conventional systems. The repair team finishes their work and then the administrator marks the status as PENDING_COMMUNITY_REVIEW which is shown in Fig.6 and Fig.7.

1. Java backend sends secure email confirmation links to the original reporter and the upvoters of that particular issue.

2. Only when a 30% of users confirmation is met by the upvoters. The issue is officially archived as RESOLVED.

3. If the users keep voting "Deny", the ticket goes to REOPENED_BY_CITIZEN.

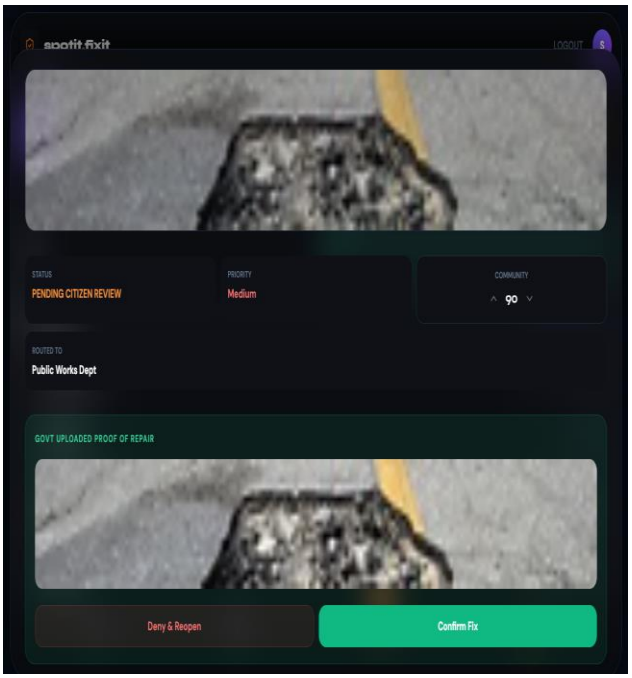

Fig. 6. Citizen-centric verification interface

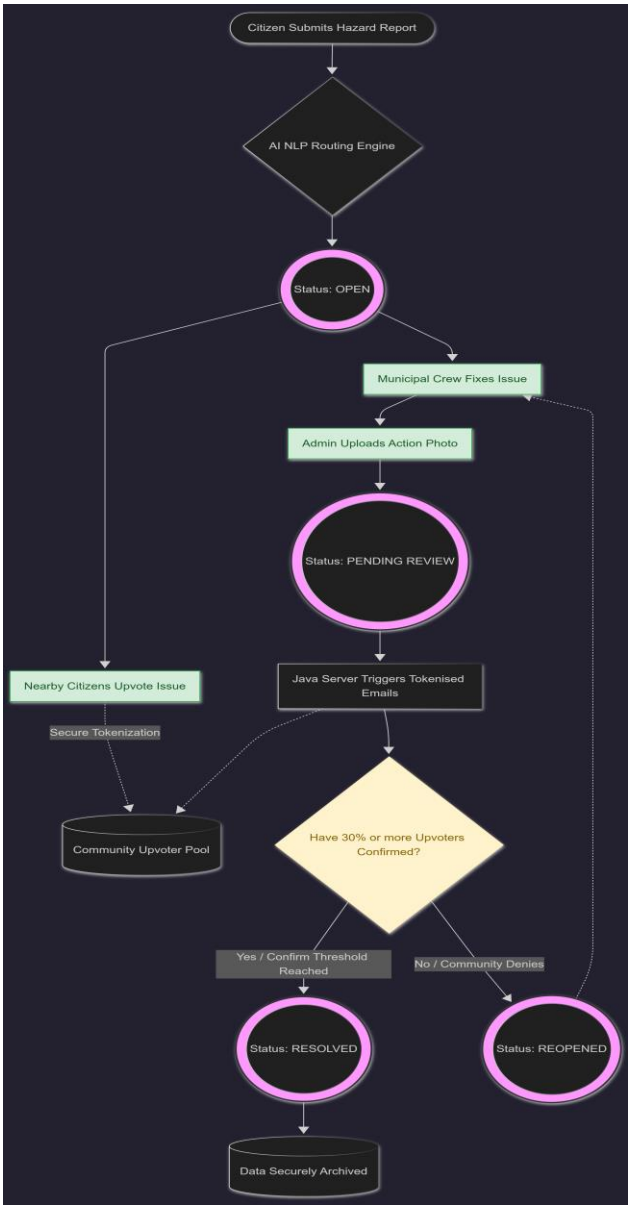

Fig. 7. The bidirectional closed-loop verification.

F. Anti-Abuse Controls

The three protective processes maintain the integrity of the reporting queue. A submission rate limiter leads to a per user 15 minute cooldown. The duplicate detection engine searches for problems within a 150m radius. This gives the option to upvote to keep the queue stand out.

IV. RESULTS AND DISCUSSION

System performance was measured in a simulated testing environment and is shown in Table II.. This was done by using

International Journal of Research in Engineering Technology and Applications
E-ISSN: 3108-2556
P-ISSN: 3108-2610

95 civic transactions like report, upvotes, and resolution attempts.

A. Routing Efficiency and Accuracy

The AI based system was able to correctly route 92. 6% reports. These were unstructured reports which were marked correctly to the municipal board without any delay.

Macro Average F-1 Score during demo: 0.92

TABLE II: NLP CATEGORISATION PERFORMANCE METRICS

Target Department	**Precision**	**Recall**	**F1-Score**
Public Works Dept	0.96	0.85	0.90
Power & Utilities	0.96	0.93	0.94
Water Supply Dept	1.00	0.96	0.98
General Routing	0.75	1.00	0.86
Overall / Macro-Avg	0.92	0.94	0.92

B. Impact on Service Level Agreements (SLAs)

Under the closed loop framework , the sort time fell from an average of 48 hours to **< 2 seconds**.

TABLE III: COMPARATIVE RESOLUTION TIMELINE ANALYSIS (SIMULATED)

Metric	**Traditional System**	**Proposed Closed-Loop**	**Improvement**
Triage & Dispatch	48 - 72 Hours	< 2 Minutes (Auto)	>99%
False Closures	~15% of cases	0% (Mathematical)	100%
Average Resolution	8.5 Days	4.2 Days	50.5%

C. Geospatial Fraud Detection Performance

Few tests were conducted on the identical photos. They were uploaded from the mock admin accounts. The duplicate image hashing algorithm gave perfect detection. It passes all 100% of the scenarios. The Haversine threshold identified all cases of spatial mismatch (distance > 0. 5 km).

D. Anti Abuse System Effectiveness

The algorithm for removing duplicate reports was very efficient. It identified the existing ticket references for all 100% of the nearby clustered test submissions. These were within a 150m radius.

V. CONCLUSION

The system offers a very good framework for ensuring civic accountability. By making it compulsory for a 30% of users conformation closed loop. The platform removes the manual sort delays, contractor side closure. This also removes the usage of old and repeated photographic evidence. Further releases will consider usage of blockchain based smart contracts. This ensures the instant disbursal of payments to contractors upon obtaining the 30% community approval.

ACKNOWLEDGMENT

The authors acknowledge the institutional support provided by Presidency University, Bengaluru. They have facilitated the research and publication of this work. This project received no external funding. The authors declare no conflict of interest.

REFERENCES

[1] E. Russell, A. Switzer and D. Edelson, "National Geographic FieldScope: A Collaboratory Geospatial Platform for Citizen Science," 2011 IEEE Seventh International Conference on e-Science Workshops, Stockholm, Sweden, 2011, pp. 34-38, doi: 10.1109/eScienceW.2011.24.

[2] O. B. Mora, R. Rivera, V. M. Larios, J. R. Beltrán-Ramírez, R. Maciel and A. Ochoa, "A Use Case in Cybersecurity based in

Blockchain to deal with the security and privacy of citizens and Smart Cities Cyberinfrastructures," 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 2018, pp. 1-4, doi: 10.1109/ISC2.2018.8656694.

[3 N. M. Kumar, S. Goel and P. K. Mallick, "Smart cities in India: Features, policies, current status, and challenges," 2018 Technologies for Smart-City Energy Security and Power (ICSESP), Bhubaneswar, India, 2018, pp. 1-4, doi: 10.1109/ICSESP.2018.8376669.

[4] P. HoražĎovský and M. Prokýšek, "Proposal of the Successful Process of Implementing Smart City Designs into a real City," 2023 Smart City Symposium Prague (SCSP), Prague, Czech Republic, 2023, pp. 1-6, doi: 10.1109/SCSP58044.2023.10146232.

[5] A. Gayen, V. Mehta, M. Sen, U. Chowduray and A. Jana, "Destiny of Legal Petition: Accept or Reject?: A Machine Learning Approach to Predict the Legal Petition's Initial Decision," 2024 IEEE Region 10 Symposium (TENSYMP), New Delhi, India, 2024, pp. 1-6, doi: 10.1109/TENSYMP61132.2024.10752269.

[6] E. Mardacany, "Smart cities characteristics: importance of buit environments components," IET Conference on Future Intelligent Cities, London, 2014, pp. 1-6, doi: 10.1049/ic.2014.0045.

[7] R. K. Das and H. Misra, "Smart city and E-Governance: Exploring the connect in the context of local development in India," 2017 Fourth International Conference on eDemocracy & eGovernment (ICEDEG), Quito, Ecuador, 2017, pp. 232-233, doi: 10.1109/ICEDEG.2017.7962540.

[8] R. Hema, S. Yousuff, P. P. Kothari, A. Anandaraj, A. Rani and C. J. Raman, "Hybrid Blockchain-Cloud Architecture for Secure e-Governance Solutions," 2025 Tenth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 2025, pp. 1-10, doi: 10.1109/ICONSTEM65670.2025.11374858.

[9] G. Ágoston, F. Pongrácz, K. G. Horváth and Z. Bukodi, "Vertical farms and smart cities – identification of common research areas, Tungsram's experience and vision in Central Europe," 2022 Smart City Symposium Prague (SCSP), Prague, Czech Republic, 2022, pp. 1-5, doi: 10.1109/SCSP54748.2022.9792542.

[10] E. H. Houssein, M. A. Othman, W. M. Mohamed and M. Younan, "Internet of Things in Smart Cities: Comprehensive Review, Open Issues, and Challenges," in IEEE Internet of Things Journal, vol. 11, no. 21, pp. 34941-34952, 1 Nov.1, 2024, doi: 10.1109/JIOT.2024.3449753.

[11 A. Hayar and G. Betis, "Frugal social sustainable collaborative smart city casablanca paving the way towards building new concept for "future smart cities by and for all"," 2017 Sensors Networks Smart and Emerging Technologies (SENSET), Beiriut, Lebanon, 2017, pp. 1-4, doi: 10.1109/SENSET.2017.8305444.

[12] H. Ali, R. Qazi and M. A. Shah, "Smart Cities: Methods, Encounters & Hunt for Future - Survey," 2019 25th International Conference on Automation and Computing (ICAC), Lancaster, UK, 2019, pp. 1-6, doi: 10.23919/IConAC.2019.8895019.

[13] J. Cheng, N. Gould, L. Han and C. Jin, "Big Data for Urban Studies: Opportunities and Challenges: A Comparative Perspective," 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Toulouse, France, 2016, pp. 1229-1234, doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0189.

[14] Y. Xu et al., "Rethinking the Effect of Sparse Data Completion on Sparse Mobile Crowdsensing Tasks," in IEEE Transactions on Mobile Computing, vol. 24, no. 6, pp. 5094-5105, June 2025, doi: 10.1109/TMC.2025.3531362.

[15] J. Murray and B. Lagesse, "Toward Easier Development of Privacy-Preserving Mobile Crowdsensing Applications," 2025 26th IEEE International Conference on Mobile Data Management (MDM), Irvine, CA, USA, 2025, pp. 264-269, doi: 10.1109/MDM65600.2025.00058.

[16] J. Zhang, J. Ma, W. Wang and Y. Liu, "A novel privacy protection scheme for participatory sensing with incentives," 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, Hangzhou, China, 2012, pp. 1017-1021, doi: 10.1109/CCIS.2012.6664535.

[17] A. P. Kartin, H. Tampubolon and H. Sutrisno, "Exploring Urban Traffic: Uncovering Sectional Anomalies through an Optimization Framework," 2024 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, 2024, pp. 566-570, doi: 10.1109/IEEM62345.2024.10856983.

[18] S. Lin, J. Chen, J. Han, D. Chen and S. Su, "Simulation of WiFi Fingerprint Location Model Based on Weighted K Nearest Neighbor Algorithm," 2023 International Conference on Telecommunications, Electronics and Informatics (ICTEI), Lisbon, Portugal, 2023, pp. 364-369, doi: 10.1109/ICTEI60496.2023.00163.

[19] C. Ou, Y. Zhan and Y. Chen, "Identifying Malicious Players in GWAP-based Disaster Monitoring Crowdsourcing System," 2019 2nd International Conference on Artificial Intelligence and Big Data

(ICAIBD), Chengdu, China, 2019, pp. 369-378, doi: 10.1109/ICAIBD.2019.8836972.

[20] P. Omrani, Z. Ebrahimian, R. Toosi and M. A. Akhaee, "Bilingual COVID-19 Fake News Detection Based on LDA Topic Modeling and BERT Transformer," 2023 6th International Conference on Pattern Recognition and Image Analysis (IPRIA), Qom, Iran, Islamic Republic of, 2023, pp. 01-06, doi: 10.1109/IPRIA59240.2023.10147179.

[21] E. Cambria and B. White, "Jumping NLP Curves: A Review of Natural Language Processing Research [Review Article]," in IEEE Computational Intelligence Magazine, vol. 9, no. 2, pp. 48-57, May 2014, doi: 10.1109/MCI.2014.2307227.

[22] G. Jin, "Application Optimization of NLP System under Deep Learning Technology in Text Semantics and Text Classification," 2022 International Conference on Education, Network and Information Technology (ICENIT), Liverpool, United Kingdom, 2022, pp. 279-283, doi: 10.1109/ICENIT57306.2022.00068.

[23] S. B. Shah, S. A. Pahune, V. Prajapati and M. Menghnani, "Efficient NLP-Based Framework for Tweets Sentiment Analysis via Advanced Machine Learning Model," 2025 Global Conference in Emerging Technology (GINOTECH), PUNE, India, 2025, pp. 1-6, doi: 10.1109/GINOTECH63460.2025.11076911.

[24] S. Prabowo et al., "Privacy-Preserving Tools and Technologies: Government Adoption and Challenges," in IEEE Access, vol. 13, pp. 33904-33934, 2025, doi: 10.1109/ACCESS.2025.3540878.

[25] H. Jiang, J. Pei, D. Yu, J. Yu, B. Gong and X. Cheng, "Applications of Differential Privacy in Social Network Analysis: A Survey," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 1, pp. 108-127, 1 Jan. 2023, doi: 10.1109/TKDE.2021.3073062.

[26] S. Amjad, S. Craß, A. Taudes and D. Svetinovic, "Privacy and Security Requirements Challenges in Blockchain-Based Decentralized Federated Learning," 2024 IEEE 32nd International Requirements Engineering Conference Workshops (REW), Reykjavik, Iceland, 2024, pp. 348-352, doi: 10.1109/REW61692.2024.00053.

[27] X. Shen, C. Xu, L. Zhu, R. Lu, Y. Guan and X. Zhang, "Blockchain-Based Lightweight and Privacy-Preserving Quality Assurance Framework in Crowdsensing Systems," in IEEE Internet of Things Journal, vol. 11, no. 1, pp. 974-986, 1 Jan.1, 2024, doi: 10.1109/JIOT.2023.3288349.

[28] Shen Haibo and Hong Fan, "A context-aware role-based access control model for Web services," IEEE International Conference on e-Business Engineering (ICEBE'05), Beijing, China, 2005, pp. 220-223, doi: 10.1109/ICEBE.2005.1.

[29] X. Huang, H. Wang, Z. Chen and J. Lin, "A Context, Rule and Role-Based Access Control Model In Enterprise Pervasive Computing Environment," 2006 First International Symposium on Pervasive Computing and Applications, Urumqi, China, 2006, pp. 497-502, doi: 10.1109/SPCA.2006.297443.

[30] S. Chopvitayakun, M. Rattanasiriwongwut and M. Ketcham, "An Integration of User-Centered Design and Design Thinking Principles for Developing a Mobile Application for Nutritional Tracking for Thai Elderly: A Mixed-Method Study," 2025 IEEE International Conference on Cybernetics and Innovations (ICCI), Chonburi, Thailand, 2025, pp. 1-6, doi: 10.1109/ICCI64209.2025.10987228.

[31] P. Mykytyn, M. Brzozowski, Z. Dyka and P. Langendoerfer, "GPS-Spoofing Attack Detection Mechanism for UAV Swarms," 2023 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2023, pp. 1-8, doi: 10.1109/MECO58584.2023.10154998.

[32] M. Allahbakhsh, B. Benatallah, A. Ignjatovic, H. R. Motahari-Nezhad, E. Bertino and S. Dustdar, "Quality Control in Crowdsourcing Systems: Issues and Directions," in IEEE Internet Computing, vol. 17, no. 2, pp. 76-81, March-April 2013, doi: 10.1109/MIC.2013.20.