International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 12, Issue 12, December 2023)

Empowering Crowdsourcing: Advantages of Implementing a Robust Digital Privacy Framework: A Comprehensive Review

Santosh Kumar[1], Dr. Mohammad Faisal[2]
[1]*Research Scholar,* [2]*Professor & Head, Department of Computer Application, Integral University, Lucknow, India*
[1]sanb2@rediffmail.com, [2]mdfaisal@iul.ac.in

***Abstract*-- Through the utilisation of varied participants' collective intelligence, crowdsourcing has become a strong paradigm in the ever-changing field of collaborative problem-solving and knowledge generating. In this extensive examination, this review article looked at all the different ways crowdsourcing works, but this study focuses in particular on how digital privacy frameworks affect how successful and long-lasting crowdsourced projects are. To maintain participant confidence and long-term engagement in ever-increasing crowdsourcing projects, it is critical to resolve privacy problems. The assessment delves into the difficulties, resources, and technology necessary for coordinating crowdsourced projects, such as blockchain and machine learning algorithms. By focusing on the regulatory, ethical, and legal aspects, it presents a synthesis of digital privacy frameworks designed to meet the needs of crowdsourcing. Enhanced participant trust, legal compliance, and resistance against data breaches are all benefits that may be thoroughly explained by a solid digital privacy framework. This review adds significantly to the ongoing conversation about crowdsourcing privacy and helps us better grasp its critical function in collaborative problem-solving and knowledge-generation.**

***Keywords*-- Crowdsourcing, Digital Privacy Framework, Blockchain, Legal Compliance.**

I. INTRODUCTION

In the contemporary landscape of collaborative information generation and problem-solving, crowdsourcing has emerged as a powerful paradigm, harnessing the collective intelligence of diverse participants. However, the efficacy of crowdsourcing is contingent upon the assurance of privacy for both contributors and requesters, an imperative addressed by the implementation of a robust digital privacy framework (Ang, Seng and Ngharamike, 2022). This comprehensive review endeavours to scrutinize the manifold advantages associated with the establishment of such frameworks in the domain of crowdsourcing. (Brabham, 2008)

Crowdsourcing, as a mechanism for obtaining solutions, ideas, or information from a broad and distributed pool of contributors, is ubiquitously employed across various domains, including but not limited to data annotation, image recognition, and problem-solving (Wang *et al.*, 2017). As the magnitude and complexity of crowdsourced endeavours escalate, concerns regarding the privacy and confidentiality of the involved stakeholders become increasingly salient. A robust digital privacy framework stands as an indispensable bulwark against potential breaches, ensuring the protection of sensitive information and fostering an environment of trust (Fan and Yang, 2022).

The review unfolds by delving into the multifaceted challenges encountered in the realm of crowdsourcing, emphasizing the critical role of privacy as a linchpin for sustained participation. Contributors, drawn from disparate geographical locations and cultural backgrounds, inherently entrust their data and intellectual contributions to the crowdsourcing platform (Nguyen, Jung and Hwang, 2020). Consequently, addressing privacy concerns becomes paramount to mitigating risks associated with data misuse, identity exposure, and the erosion of trust among participants.

In light of the expansion and variety of crowdsourcing platforms, this work provided a comprehensive overview of the current tools and technology that are essential for coordinating crowdsourced projects. In order to strengthen the privacy posture of crowdsourcing ecosystems, we go beyond the basic data gathering and dissemination task and investigate modern technologies like blockchain processes and machine learning algorithms.

The most important part of this research reveals a digital privacy framework that has been synthesized and is designed to meet the needs of crowdsourcing. To emphasize how important, it is to set up privacy-centric architectures, we thoroughly analyzed existing frameworks and proposed an adaptable, all-encompassing approach (Zhang *et al.*, 2020).

The framework envisages a seamless integration of technology and policy-driven strategies to protect participants' privacy and integrity by exploring the legal, ethical, and regulatory aspects.
Hence, this paper reviews the various advantages and benefits of implementing the digital privacy framework in crowdsourcing.

II. Literature Review

The term "crowdsourcing" is used to refer to the practise by which institutions and organisations acquire external resources to complete duties that were first performed internally. This is accomplished on the premise that anyone can obtain valuable information. (Hossain and Kauranen, 2015)(Alizadeh, 2018)(Liu, 2017), numerous authors reference the work of (Estellés-Arolas and González-Ladrón-De-Guevara, 2012), who looked for points where various definitions of crowdsourcing overlapped and didn't overlap in order to create a single definition that covered all types of crowdsourcing. In addition to three components, the authors enumerate eight functions of crowdsourcing: (a) The structure of a crowd, including its composition, functions, and reciprocal benefits; (b) The initiator: its identity and the reciprocal benefit it obtains; (c) approach: the nature of the process, the format of the call, and the medium employed.

Crowdsourcing, as used in local government, is using cutting-edge technologies to gather public input to find solutions that organisations and specialised groups previously identified (Bertot, Jaeger and Hansen, 2012). (Loukis, Charalabidis and Androutsopoulou, 2017) and (Spiliotopoulou *et al.*, 2014), Crowdsourcing can be categorised as either active or passive. Active crowdsourcing is a process whereby the government disseminates information regarding a public policy issue or problem with the intention of soliciting opinions or potential solutions. Passive crowdsourcing transpires when governmental entities surveil social platforms through the extraction and analysis of user-generated content.

By exploring the knowledge of citizens, crowdsourcing attempts to mobilise the expertise that is dispersed in a variety of ways to develop or enhance public policies (Chris Zhao and Zhu, 2014) and services that are more practical, balanced, and relevant to social issues. (Spiliotopoulou *et al.*, 2014).

Pervasive systems, which rely on contextual information to perform at their best, have recently become more popular and in high demand due to technological advancements.

While there is a lot of literature on context-aware systems, most of it has ignored the semantic-based approach to crowdsourcing. Because of this, it suggests problems with reasoning control mechanism representation, context, and service acquisition (Abdulsalam, Muhammad and Mohamed, 2023) examined a framework for reasoning based on semantics, with an emphasis on the field of mobile crowdsourcing. Extrinsic or intrinsic, various domains learn different kinds of context. Using the evaluated frameworks as inspiration, a process framework was constructed incorporating the critical element for context-aware reasoning and employing a semantic approach. The framework has two potential applications: one is in the realm of context-aware mobile crowdsourcing, and the other is in the realm of reasoning control. One thing that sets it apart from other crowdsourcing frameworks is its emphasis on representation of the acquired information, in addition to context and service acquisition.

In this work, (Thakur and Marchang, 2023) conducted an analysis of different methods and approaches to mobile crowd sensing (MCS) security and privacy. They begin by going over some of the generic MCS architecture's security and privacy concerns at various points. After that, they looked at different MCS general-purpose privacy architectures and compared them. Among other privacy-related topics, they address task delegation, incentive systems, data aggregation, truth finding, and data reporting.

According to (Kodjiku *et al.*, 2023), Platforms for crowdsourcing are crucial in achieving the objectives of reducing costs and resource consumption through increasing transparency and fostering collaborative involvement among participants. To achieve this objective, these platforms are equipped with tools that can track and assess employees' performance. But there are still major roadblocks. Issues with trust arise with centralised systems due to their vulnerability to assaults that target a single point of failure. Additionally, the implementation of biassed evaluations and the distribution of incentives may lead to a decline in employee motivation, and the manipulation of data by malevolent actors weakens trust in the assessment process. Consequently, a decentralised system that ensures trustworthiness, tamper-resistance, accountability, dependability, transparency, and security is required to meet these challenges. This study introduces a safe, multi-tiered crowdsourcing architecture for worker quality evaluations using blockchain technology. A three-tier paradigm that incorporates the Identity, Worker Activity, and Reputation levels is employed by WQCrowd. The software additionally makes use of smart contracts.

The accuracy of performance reviews has also been improved with the addition of an automated game-based worker evaluation technique. As a result of our PoC (Proof of Concept) study, (Kodjiku *et al.*, 2023) demonstrated that the use of the blockchain system successfully resolves security issues, such as privacy, accountability, and trust, that are common in the present methods used to assess employee performance. Moreover, our proposed method is able to make educated decisions about worker quality performance evaluations thanks to the game-based automated system.

In (Tan et al., 2022) focused on three important areas of digital strategies to increase community involvement in clinical trials: digital crowdsourcing to build trial components, digital technology for trial processes to decentralise trials, and digital qualitative research methodologies. Specifically, they show how digital methods decentralised research procedures, which increased community engagement, and how digital techniques increased diversity of participants, which promoted community engagement. Along with outlining possible benefits, drawbacks, and practical considerations, they talk about the new opportunities that digital technology give for community engagement. Science maintains that better health outcomes and more equity can result from bolstering community engagement through digital means.

In this study, (Kim, Edemacu and Jang, 2022) investigate in depth the current methods for securing MCS employees' location privacy. The researchers compared the location protection systems from three different angles: architecture, privacy, computational overhead, and utility. They did this based on the algorithms' characteristics. Recent developments in communication and sensor technology have made mobile crowdsensing (MCS), already one of the most effective crowdsourcing applications, an even more potent weapon in the fight against scalable and complicated sensing challenges. In most cases, MCS is a kind of location-aware crowdsourcing wherein workers are required to physically go to a designated spot in order to finish tasks. This means that employees have an obligation to tell service providers their exact whereabouts at all times. Due to privacy concerns, however, most employees are hesitant or uncomfortable providing service providers with their precise location data. This is because location information may contain sensitive data. Many consider this to be the biggest obstacle that MCS must overcome. In order to encourage more people to take part in MCS, it is crucial to ensure that their location remains private.

There have been a plethora of studies in recent years aimed at safeguarding the location privacy of MCS participants. Additionally, in order to encourage additional research in this field, scholars deliberated on some encouraging avenues for future study.

In (Shahrour and Xie, 2021) examined how crowdsourcing and the Internet of Things (IoT) play a part in building smart cities. The review of the literature demonstrates that the scientific community is becoming more and more concerned about these three issues and how they relate to the promotion of urban development. The paper first introduces the concept of smart cities, focusing on data's role in smart city solutions and smart city architecture, based on a thorough review of the literature. The Internet of Things is presented in the second section with an emphasis on security, smart city applications, and IoT technology. Finally, crowdsourcing is covered in the study, with a focus on mobile crowdsourcing and how it might be applied to smart cities. This research shows that crowdsourcing and the IoT have a significant effect on the data collecting and services layers, which are pillars of smart city apps. Both levels ensure the merging of the digital and physical realms, making them the primary pillars upon which smart city projects rest. According to the reviewed literature, smart city citizen-centered research focuses on crowdsourcing, while smart city technology-centered research mainly examines the Internet of Things. Nevertheless, both types of research must work together more closely to advance smart city development. Crowdsensing is a relatively new area that mixes crowdsourcing with the Internet of Things; this partnership might improve upon recent developments in the area.

In (Yfantis et al., 2020) contribute to the exploration of crowdsourcing's usage in the public sector by tracings its conceptual structure, application's advantages and potential adoption from the government's or the citizen's side. A systematic narrative literature review is the suggested method, which captures the latest trends of crowdsourcing by diving the existing bibliography into thematic categories and analysing the findings. The study resulted in the suggestion of new elements for the definition of crowdsourcing, including privacy, big data, political will and other important aspects. Moreover, the current academic work discusses the advantages of crowdsourcing in the public sector such as cost reduction, decision making, public issues monitoring in real time, etc. At last, this paper argues about the adoption of crowdsourcing and the obvious issues such as lack of trust, crowdsourcing's importance for the public servants and other serious subjects.

The academic and non-academic communities both make heavy use of crowdsourcing platforms like Amazon Mechanical Turk (MTurk), but the risks and difficulties associated with crowdsourcing in terms of privacy have received little attention. In order to contribute to the field's progress in crucial new directions, (Xia and McKernan, 2020) first examines the privacy risks associated with various forms of crowdsourcing using Brabham's crowdsourcing typology and Solove's privacy taxonomy. The study then delves into the privacy issues raised by the features of the crowdsourcing platform, requesters, workers, and tasks. These privacy issues are examined and divided into two groups: theoretical and practical. Based on the review and discussion, (Xia and McKernan, 2020) proposed methods to understand and address crowdsourcing privacy issues. Presenting future research implications concludes the paper.

In a survey conducted by (Lalit and Reddy, 2018), Survey data from 229 participants is used to analyze the opportunities and challenges in crowdsourcing security. The findings shed light on what drives participation, what controls quality, and where work needs to be done. "Software development and testing," which comprises information sharing, and "question and answers" A bug Notwithstanding their concerns regarding information security and privacy, security experts have identified bounty as the top crowdsourcing task. 'Credibility' of the contributors is one of the quality attributes that was analyzed and found to be a critical area for improvement and increased crowdsourcing participation.

In this work, (Balicki, Jerzy and Brudo, Piotr and Szpryngier, 2014) novel approach that integrates crowdsourcing and volunteer computing is introduced. A comprehensive description, analysis, and comparison are provided of two web computing paradigms: volunteer computing and grid computing. The attributes of BOINC and its impact on worldwide Internet processing are demonstrated through the emphasis placed on the applications it can enable and the challenges it can resolve. A practical demonstration of diverse applications and an examination of the distributed processing capabilities of Comcute, an alternative grid computing system developed at the Gdansk University of Technology, are included in the presentation.

III. Conclusion

Crowdsourcing has become a powerful paradigm in the constantly changing field of collaborative problem-solving and knowledge development.

This extensive research has explored all aspects of crowdsourcing, but it has zeroed in on the critical role that digital privacy standards play in determining the success or failure of crowdsourced projects.

In order to maintain the trust and ongoing involvement of contributors, it is crucial to address privacy concerns, especially with the growing size and complexity of crowdsourced activities. An essential measure to prevent possible breaches and the loss of participant confidence is the establishment of a strong digital privacy framework, since contributors from all over the world and all walks of life are putting their intellectual capital into crowdsourcing platforms.

The review painstakingly negotiated the complexities of crowdsourcing, highlighting the importance of anonymity as a key to long-term engagement. We looked at the many tools and technologies that are essential to crowdsourcing activity orchestration, in addition to the issues that come with it. This review looked at how modern technologies, such as blockchain and machine learning algorithms, could improve crowdsourcing environments' privacy protections.

The review's main contribution is the digital privacy framework it synthesises and adapts to the needs of crowdsourcing. By thoroughly examining existing frameworks and suggesting an adaptable, all-encompassing paradigm, the paper highlights the need of privacy-centric designs. Protecting participants' privacy and integrity is the goal of the framework's technical and policy-driven efforts, which aim to harmonise with one another across legal, ethical, and regulatory domains.

The benefits of establishing such a strong digital privacy framework were thoroughly explained, covering ground such as increased confidence among participants, conformity with regulations, and resistance to data breaches. Thorough analysis was conducted on every aspect, proving that strong privacy measures affect the success and durability of crowdsourcing projects.

Finally, the purpose of this review is to add something meaningful to the current conversation on crowdsourcing privacy. It seeks to boost crowdsourcing efforts by promoting a detailed comprehension of the critical role of digital privacy frameworks, strengthening the groundwork for collaborative knowledge creation and problem-solving in an era that is more linked and data-driven. The importance of digital privacy cannot be overstated as new technologies transform crowdsourcing. As technological advancements continue to shape the landscape of crowdsourcing, the imperatives of digital privacy must remain at the forefront, guiding the evolution of ethical and effective collaborative practices.

REFERENCES

[1] Abdulsalam, N.H., Muhammad, S. and Mohamed, R. (2023) 'A Review of Semantic-Based Reasoning Framework for Context-Aware Mobile-Crowdsourcing', in 2023 13th International Conference on Information Technology in Asia (CITA), pp. 94–99. Available at: https://doi.org/10.1109/CITA58204.2023.10262576.

[2] Alizadeh, T. (2018) 'Crowdsourced Smart Cities versus Corporate Smart Cities', in IOP Conference Series: Earth and Environmental Science. Available at: https://doi.org/10.1088/1755-1315/158/1/012046.

[3] Ang, K.L.M., Seng, J.K.P. and Ngharamike, E. (2022) 'Towards Crowdsourcing Internet of Things (Crowd-IoT): Architectures, Security and Applications', Future Internet [Preprint]. Available at: https://doi.org/10.3390/fi14020049.

[4] Balicki, Jerzy and Brudo, Piotr and Szpryngier, P. (2014) 'Crowdsourcing and Volunteer Computing as Distributed Approach for Problem Solving', Applications of Information Systems in Engineering and Bioscience : Proceedings of the 13th International Conference on Software Engineering, Parallel and Distributed Systems, 14, pp. 115–121.

[5] Bertot, J.C., Jaeger, P.T. and Hansen, D. (2012) 'The impact of polices on government social media usage: Issues, challenges, and recommendations', Government Information Quarterly [Preprint]. Available at: https://doi.org/10.1016/j.giq.2011.04.004.

[6] Brabham, D.C. (2008) 'Crowdsourcing as a model for problem solving: An introduction and cases', Convergence [Preprint]. Available at: https://doi.org/10.1177/1354856507084420.

[7] Chris Zhao, Y. and Zhu, Q. (2014) 'Effects of extrinsic and intrinsic motivation on participation in crowdsourcing contest', Online Information Review [Preprint]. Available at: https://doi.org/10.1108/oir-08-2014-0188.

[8] Estellés-Arolas, E. and González-Ladrón-De-Guevara, F. (2012) 'Towards an integrated crowdsourcing definition', Journal of Information Science [Preprint]. Available at: https://doi.org/10.1177/0165551512437638.

[9] Fan, S. and Yang, Z. (2022) 'Safety and security co-analysis in transport systems: Current state and regulatory development', Transportation Research Part A: Policy and Practice [Preprint]. Available at: https://doi.org/10.1016/j.tra.2022.11.005.

[10] Hossain, M. and Kauranen, I. (2015) 'Crowdsourcing: A comprehensive literature review', Strategic Outsourcing [Preprint]. Available at: https://doi.org/10.1108/SO-12-2014-0029.

[11] Kim, J.W., Edemacu, K. and Jang, B. (2022) 'Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey', Journal of Network and Computer Applications [Preprint]. Available at: https://doi.org/10.1016/j.jnca.2021.103315.

[12] Kodjiku, S.L. et al. (2023) 'WQCrowd: Secure blockchain-based crowdsourcing framework with multi-tier worker quality evaluation', Journal of King Saud University - Computer and

[13] R Singh, PK Mannepalli Journal of Advanced Research Engineering and, 2020, Cloud Malicious Threat Detection By Features From Intelligent Water Drop Set And EBPN, 2021 5th International Conference on Information Systems and Computer Networks (ISCON), DOI: 10.1109/ISCON52037.2021.9702492

[14] Mannepalli, P.K., Kulurkar, P., An Enhanced Classification Model for Depression Detection Based on Machine Learning with Feature Selection Technique DOB :10.1109/ISCON52037.2021.9702492.

[15] Rashmi Singh; Praveen Kumar Mannepalli, Invasive Weed optimization Algorithm Based Trained Neural Network for Cloud Malicious Threat Detection, 2021 IEEE International Conference on Technology, Research, and Innovation for Betterment of Society (TRIBES), 10.1109/TRIBES52498.2021.9751674.

[16] Deepak Kumar Rathore;Praveen Kumar MannepalliA Review of Machine Learning Techniques and Applications for Health Care2021 International Conference on Advances in Technology, Management & Education (ICATME), DOI: 10.1109/ICATME50232.2021.9732761.

[17] Ankur Pandey; Ankur Chaturvedi; Manish Gupta; Praveen Kumar Mannepalli, An Automated Face Mask Detection System using Deep CNN on AWS Cloud Infrastructure, 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), DOI: 10.1109/ICESC57686.2023.10193710.

[18] K. Anil; Praveen Kumar Mannepalli, Achieving Effective Secrecy based on Blockchain and Data Sharing in Cloud Computing, 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), DOI: 10.1109/CSNT51715.2021.9509663.

[19] Praveen Kumar Mannepalli; Devendra Singh Kushwaha, Face Recognition Based on Cascade Classifier Using Deep Learning, 2023 1st International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP), DOI: 10.1109/IHCSP56702.2023.10127172

[20] Praveen Kumar Mannepalli; Parcha Kalyani; An Early Detection of Pneumonia in CXR Images using Deep Learning Techniques, 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), DOI: 10.1109/ICIDCA56705.2023.10100230

[21] Information Sciences, 35(10), p. 101843. Available at: https://doi.org/https://doi.org/10.1016/j.jksuci.2023.101843.

[22] Lalit, M.S. and Reddy, Y.R. (2018) 'Crowdsourcing security: Opportunities and challenges', in Proceedings - International Conference on Software Engineering. Available at: https://doi.org/10.1145/3195836.3195862.

[23] Liu, H.K. (2017) 'Crowdsourcing Government: Lessons from Multiple Disciplines', Public Administration Review [Preprint]. Available at: https://doi.org/10.1111/puar.12808.

[24] Loukis, E., Charalabidis, Y. and Androutsopoulou, A. (2017) 'Promoting open innovation in the public sector through social media monitoring', Government Information Quarterly [Preprint]. Available at: https://doi.org/10.1016/j.giq.2016.09.004.

[25] Nguyen, L.V., Jung, J.J. and Hwang, M. (2020) 'Ourplaces: Cross-cultural crowdsourcing platform for location recommendation services', ISPRS International Journal of Geo-Information [Preprint]. Available at: https://doi.org/10.3390/ijgi9120711.

[26] Shahrour, I. and Xie, X. (2021) 'Role of internet of things (IoT) and crowdsourcing in smart city projects', Smart Cities [Preprint]. Available at: https://doi.org/10.3390/smartcities4040068.

[27] Spiliotopoulou, L. et al. (2014) 'A framework for advanced social media exploitation in government for crowdsourcing', Transforming Government: People, Process and Policy [Preprint]. Available at: https://doi.org/10.1108/TG-01-2014-0002.

[28] Tan, R.K.J. et al. (2022) 'Digital approaches to enhancing community engagement in clinical trials', npj Digital Medicine[Preprint]. Available at: https://doi.org/10.1038/s41746-022-00581-1.

[29] Thakur, T. and Marchang, N. (2023) 'A review of security and privacy approaches in mobile crowd sensing', in AIP Conference Proceedings. Available at: https://doi.org/10.1063/5.0133334.

[30] Wang, Y. et al. (2017) 'Mobile crowdsourcing: framework, challenges, and solutions', in Concurrency and Computation: Practice and Experience. Available at: https://doi.org/10.1002/cpe.3789.

[31] Xia, H. and McKernan, B. (2020) 'Privacy in Crowdsourcing: a Review of the Threats and Challenges', Computer Supported Cooperative Work: CSCW: An International Journal [Preprint]. Available at: https://doi.org/10.1007/s10606-020-09374-0.

[32] Yfantis, V. et al. (2020) 'A systematic literature review of the crowdsourcing in the public sector', in.

[33] Zhang, Z. et al. (2020) 'A crowdsourcing method for online social networks security assessment based on human-centric computing', Human-centric Computing and Information Sciences [Preprint]. Available at: https://doi.org/10.1186/s13673-020-00230-0.