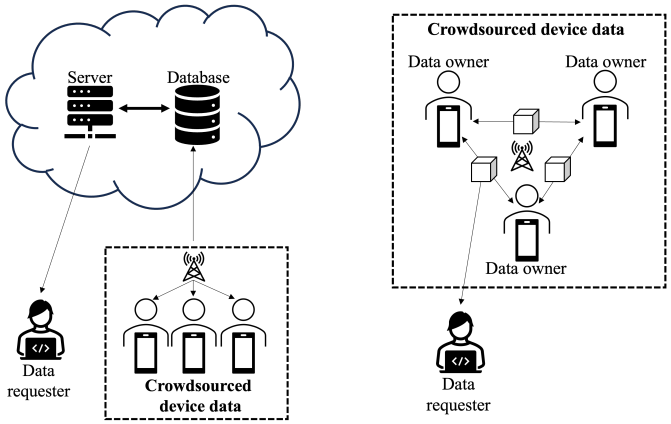
Towards a Regulation Compliant Crowdsourcing Mechanism in XG through Multichain-Blockchain

Maninderpal Singh*, William Bjorndahl*, Amritpal Singh†, Joseph Camp*
*Electrical and Computer Engineering Department, Southern Methodist University, Dallas, USA
†Department of Computer Science, Durham University, United Kingdom
Email: maninderpals@smu.edu, wbjorndahl@smu.edu, amritpal.singh@durham.ac.uk, camp@smu.edu

2024 IEEE International Conference on Communications Workshops (ICC Workshops) | 979-8-3503-0405-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCWORKSHOPS59551.2024.10615849

***Abstract*—The collection and processing of data is vital in almost all domains of current and future technological developments and their sustainability. Wireless communication technologies are no exception to this and over the years substantial work has been done in this domain to achieve better data rates and better coverage areas. In real-time systems where wireless networks work, the number of interdependent factors is numerous making the simulated environments restricted for performance analysis and tweaking. Hence, crowdsourcing becomes a very suitable candidate for the collection of data for various underlying purposes especially in the future generation called XG of wireless technologies. But, crowdsourcing has various challenges one of which is to ensure the system is compliant with various international policies for data collection storage, and processing guidelines. In this proposed ecosystem, a blockchain-based transparent logic and data crowdsourcing mechanism is used. The use of multichain blockchains is explored to find the viability and experiment with challenges in performing the same. The proposed underlying mechanisms are subjected to various use cases related to compliance rules. The evaluations support the viability of the proposed system to be explored at a large scale.**

***Index Terms*—crowdsourcing, multichain, blockchain, GDPR, compliance, erasable blockchain, controllable sharing**



(a) Cloud-based crowdsourcing (b) BC-based crowdsourcing

Fig. 1: Overview of a crowdsourcing framework to collect wireless cellular data using (a) cloud-based crowdsourcing and (b) blockchain-based crowdsourcing techniques.

I. Introduction

Wireless cellular communications technologies evolved greatly in the past, currently latest commercially deployed is the 5G. Whether it comes to improving the existing 5G or developing next generations (XG) of technologies, one key ingredient is always necessary i.e. data. The data is required for different purposes like monitoring network performance, evaluating the user experience of services, traffic patterns, device/hardware data, environmental and geographical data, regulatory compliance data, and security and privacy-related data. Some of the prominent methods to obtain such types of data are controlled laboratory experimentation, conducting in-field trials and development of pilots, simulation tools for virtual network modeling, collaborating with service providers to access legacy data, deploying sensor networks to monitor wireless communication parameters, community-based structural testing programs, regulatory reports, and surveys. However, the amount of data that can be gathered through any of these approaches can not scale to the amount of data that can be gathered through crowd-sourcing. The scale of data gathered in an uncontrolled environment is the closest researchers can get to system insights to identify limitations of the current working system and also explore solutions in actual scenarios [1].

But data gathering these days is not just collecting the data from users, it's about providing more control to the user about their data [2] e.g. UK GDPR requirements [3] lays down principles that must be followed while designing any approach for data collection. One of the key terms around which the whole system revolves is personal information. As per personal information is information that relates to an identified or identifiable individual and it needs to be dealt with utmost care. Processing and storing the data through cloud-based architecture [4] has some inherited limitations including single point of failure, limited scalability, lack of diversity, reduced trust, inflexibility, data ownership, and control concerns. Hence, in this work a decentralized framework for crowd-sourcing is explored that is capable of meeting the requirements of strict data collection and processing regulations like GDPR [5]. Among various decentralized mechanisms including interplanetary file system (IPFS), secure multi-party computation (SMPC), Tokenomics (Tks) and smart contracts (SC), a smart contract is the one that fulfills most requirements of the data collection regulations as exhibited in table I. Motivated by this further existing literature in the field is studied and summarized in section II.

TABLE I: Comparison of Decentralised Crowd-sourcing Data Techniques

	Logic Transparency	Ownership Control	Auditability	Distributed Data Storage
IPFS	No	Yes	Yes	Yes
SMPC	Yes	No	No	No
Tks	No	Yes	Yes	Yes
SC	Yes	Yes	Yes	Yes

II. Related Works

Several state-of-the-art frameworks have been proposed to date, claimed to be capable of data collection and processing through a decentralized mechanism i.e. blockchain. As every work sees the problem from a different angle and proposes solutions accordingly as highlighted in [6]. In this section, the key contributions from those works are analyzed and summarised to lay the foundation for the proposed technique. To begin with the work by Lu et al. [7], a framework named ZebraLancer is proposed in which the importance of confidentiality and anonymity is discussed for data crowd-sourcing. Authors have proposed to use a derivative of the zero-knowledge proof algorithm to bring confidentiality in the system. A mechanism for avoiding false data contributors to gain benefits is also proposed. Similarly, Han et al. [8] in their work for using blockchain for crowdsourcing highlighted the need to an incentive mechanism along with user profiling and sharing those profiles. Even this work also suggests the use of zk-SNARK for zero-knowledge proof implementation. In the work three different smart contracts are proposed for, identity, credit, and task-related functionalities.

Further, Xu et al. [9] proposed a blockchain-powered crowdsourcing mechanism with privacy preservation designed for mobile environments. The Works aims at optimizing the service request latency, providing a secure way of contributing data, and a mechanism to avoid exploitation of the reward mechanism. In another similar work in this direction by Sun et al. [10] a two-stage mechanism for privacy protection is proposed. In the first phase a differential privacy mechanism is used for hiding the location information of the crowd data contributors also referred to as workers in literature.

Sheng et al. [11] proposed a CPchain architecture for preserving the copyright of crowd-sourced data and enabling data trading. In a nutshell, the main motive behind this framework is to enable data sharing among buyers and sellers through smart contracts. Authors suggested that the data itself need not be put on the blockchain but instead can be shared through IPFS. A work by Tan et al. [12] proposed a crowd-sourcing framework for 5G-enabled smart city scenarios. The work identifies the various stages involved in the collection and processing of crowd-sourcing without the need for a central institution. In the wireless communication domain work by Feng et al. [13] makes use of blockchain for securely crowd-sourcing data in wireless IoT. The authors have focused on specific data collection modules and smart contracts in IoT scenarios.

TABLE II: Summary of Literature

	Usecase	Contributions	Privacy & Confidentiality	Sharing Control
Lu et al. [7]	Open	Privacy and Confidentiality	✓	×
Han et al. [8]	Open	Incentives	✓	×
Xu et al. [9]	Mobile	Truth and Fairness	✓	✓
Sun et al. [10]	Mobile	Differential Privacy	✓	×
Sheng et al. [11]	Open	Data Trading	✓	✓
Tan et al. [12]	Smart City	Modular Stages	✓	×
Feng at al. [13]	Wireless IoT	Smart Contracts	✓	×
Wang et al. [14]	Image Crowdsourcing	Multichain	✓	✓

Further, Wang et al. [14] proposed the use of multichain-based systems for crowdsourcing of quality-assured images. The proposed mechanism details evaluating the quality of images and dynamic pricing. Authors have used one main chain, and one sidechain for storage of images. Work by Ismailisufi et al. [15] evaluated the possibility of using private multichain systems for applications and concluded the deployability of the system. Further, the use of private blockchains is evaluated by Oliveira et al. [16] for performance in different workload scenarios.

Table II represents the tabular comparison of existing works.

A. Research Questions

From the study of various related works, some research questions (RQ) arise that need to be addressed to ensure that blockchain-based transparent and distributed systems are worthy of adaptation in the real world.

RQ1: If the data is stored on-chain, how the access control be enforced knowing that the data on public blockchains can be seen by everyone? When data is stored off-chain for the preservation of confidentiality of data, how to control and ensure the data access along with transparency?

RQ2: If the data contributor willingly wants to share the data with a limited number of other users, how the unrestricted forwarding of information be controlled?

RQ3: If a reward system is part of the crowdsourcing system, how to avoid exploitation of the system from duplicate and replicated data contributions?

RQ4: How to make the system compliant with data sharing regulations involving data confidentiality, access control, and right of deletion?

B. Contributions

Based upon the listed RQs the research is directed in a way that it yields the following contributions (C) to make the system more inclined towards compliance with governing

regulations.

C1: A multichain-based mechanism for creating a hybrid public-private blockchain ecosystem to ensure data privacy and protection.

C2: A mechanism for ownership establishment and crowdsourced data protection against manual manipulation is proposed.

C3: A solution is proposed for empowering data owners to govern the data forwarding through ownership establishment in multilevel access controlling.

C4: A mechanism to request the removal of data from the ecosystem is proposed.

III. System Model

The proposed system uses various identified entities, and interactions between these makes the system work. Hence, in this section, these entities are discussed to understand the system model better.

- **Data Owner:** In the proposed system has singleton set users ($\{O_i\} \subseteq \{O\}$) can contribute data ($\mathbb{data}$) into the system using its pseudo identity (O_i'). The pseudo-random identity is generated leveraging the properties of the hash function, known as preimage resistant and strongly collision-free. To ensure the randomization and collision-free pseudo identity space, salt is added into O_i as given in equation 1

$$O_i' \leftarrow O_i \oplus salt \oplus ME \tag{1}$$

  where salt is a pseudo-random number of equal length as O_i, and ME is the mobile equipment script signature. When the user with O_i' contributes data ($\mathbb{data}_j$), the ownership details are appended to the data to establish control over data sharing and other operations. In the proposed scheme, the data owner has full control of the data being shared and utilized within the ecosystem and whenever any critical operation like forwarding the data or using the data is made, the data owner is kept in a closed loop.
- **Mobile Equipment:** Another involved entity in the ecosystem is the mobile equipment (ME) which in this case is the primary source of crowdsourced data. The process of reading through the various available sensors on the mobile equipment is automated through integrity-enforced scripting, that makes sure, nobody can manually change the sensor readings and inject false data into the ecosystem. ME signatures are added to the $\mathbb{data}_j$ and O_i' as in equation 1. The process of forming ME is presented in equation 2

$$ME \leftarrow \mathbb{H}(script) \oplus \mathbb{S}_n \tag{2}$$

  where $\mathbb{H}(script)$ is the hashed value of the script static code part excluding data variables currently held values, and $\mathbb{S}_n$ is the manufacturer-specified serial number of mobile equipment. This helps in eliminating any wrongly fed data in the past if at any stage some equipment is found to be providing wrong data into the system. The details of the event sequence are presented in the next section.
- **Data Sender:** Once the ownership of the data is established through mapping as in equation 3, the data is sent to different entities of the system. The system is inclined towards regulatory compliance, hence the data-sending/forwarding process is carefully crafted in a way that the data sender ($S_{\mathbb{data}} \subseteq \{S\}$) complies with equation 4 and equation 5

$$\mathbb{data}_j \rightarrow O_i' \mapsto MAP(O_i' \parallel \mathbb{data}_j) \tag{3}$$

$$S_{\mathbb{data}_j} \subset \{O\} \cup \{S\} \tag{4}$$

  and,

$$S_{\mathbb{data}_j} \in MAP(O_i' \parallel \mathbb{data}_j) \tag{5}$$

  Where $S_{\mathbb{data}_j}$ is the entity attempting to send data $\mathbb{data}_j$. This relationship is enforced through a transparent logic implementation in the form of a smart contract on the mainchain as presented in the equation 7.
- **Data Receiver:** An entity in the system that receives data is regarded as a data receiver ($R_{\mathbb{data}}$). When $R\mathbb{data}$ receives data $\mathbb{data}_j$ from and $S_{\mathbb{data}_j}$, the access is recorded in both mainchain and sidechains of $O_{\mathbb{data}_j}$, $S_{\mathbb{data}_j}$ and $R_{\mathbb{data}_j}$ for the audit-ability purpose as represented in the equation

$$\forall R_{\mathbb{data}_j} \rightarrow \mathfrak{MC}(O_{\mathbb{data}_j}, S_{\mathbb{data}_j}, t_n, R_{\mathbb{data}_j}) \tag{6}$$

  where, t_n is the timestamp at which the $\mathbb{data}_j$ was shared with $R_{\mathbb{data}_j}$ by $S_{\mathbb{data}_j}$.
- **Blockchain:** The requirement to facilitate data transfer and control over the ownership needs to be governed through a transparent logic to build trust among users and enable the trustworthy audit-ability mechanism. Hence, in this work blockchain-based smart contracts are used. Further, the proposed ecosystem uses a hybrid system with a mix of public (mainchain) and private (sidechain) blockchains as discussed below:
  - Main Chain: The main chain ($\mathfrak{MC}$) is used as an anchor point where metadata from all participating users is stored and is used to interlink the data stored onto side chains with individual users. The data linking process is explained in detail in section IV. The composition of $\mathfrak{MC}$ is presented in equation 7 which uses $O_i', MAP(O_i' \parallel \mathbb{data}_j), S_{\mathbb{data}_j}, R_{\mathbb{data}_j}$ from equation 1, 4, 5 and 6 respectively.

$$\mathfrak{MC} \ni \mathfrak{meta}(O_i', S_{\mathbb{data}_j}, R_{\mathbb{data}_j}) \cdot MAP(O_i' \parallel \mathbb{data}_j) \tag{7}$$

  - Side Chain: Individual users have their data in their side chains ($\mathfrak{SC}$) which are private controlled access chains, that can only be accessed by authorized users. The composition of the sidechain is governed by equation 8 that is derived from mutually overlapping subsets of equations 1,4,5 and 6.

$$\mathfrak{SC} \ni \mathtt{data}(O_i' \cap S_{\mathtt{data}_j}(consent) \cap R_{\mathtt{data}_j}(requester) \tag{8}$$

where $S_{\mathtt{data}_j}(consent)$ is the sender of $\mathtt{data}_j$ who is forwarding the sharing consent request from $R_{\mathtt{data}_j}(requester)$ to O_i'.

The various discussed entities in this section are put into play in the form of a proposed scheme in section IV.

IV. Proposed Scheme

In this section, the technicality and working of various proposed mechanisms are discussed.

A. Integrity Enforced Scripting for Data Collection

It is vital to ensure that the data being collected and contributed by O_i' is correct and is not manually manipulated. Hence, in Phase 1 of this subsection, the mechanism for enforcing the integrity check for the script used on ME for the collection and contribution of data is depicted in figure 2.

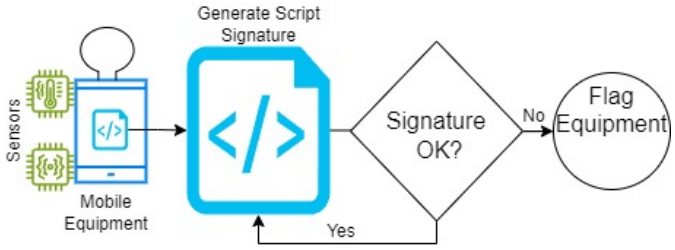


Fig. 2: Integrity Ensured Scripting for Package Creation

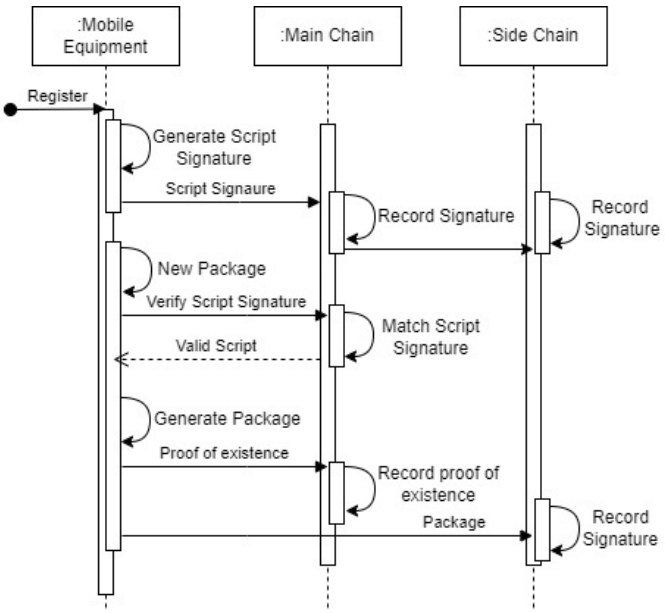


Fig. 3: Script and Package Generation Sequence Diagram

The script reads data directly from sensors, and manual updation of data is not permitted. Even if a user tries to inject false data into the script through virtual sensor sockets, the same is not permitted. To begin with, when a user downloads and registers in the ecosystem for the contribution of crowd-sourced data, the downloaded script is converted into a unique scripting signature using equation 2. The script copies are placed at $\mathfrak{MC}$ and $\mathfrak{SC}_{O_i'}$. When ME attempts to contribute some data to the ecosystem, the signatures of the script available at $\mathfrak{MC}$ and $\mathfrak{SC}_{O_i'}$ are validated first before the data is accepted and added.

Once, the phase for script validation is complete the ownership establishment phase kicks in. Here, the establishment of ownership of the content becomes very important to eliminate the possibility of users copying data from others and feeding it into the system for the exploitation of the system e.g. reward systems. For this purpose, a zero-knowledge-based protocol [17] is used in which the data contributor i.e U_i' is the prover and $\mathfrak{MC}$ and $\mathfrak{SC}$ are the challenges to establish the ownership. The sequence of steps followed through phase 1 and phase 2 are represented in figure 3

B. A case study for controlling sharing of owned data

The proposed framework handles uncontrolled data forwarding and untraced data access by different users. The challenge presented is to make the data only accessible to legitimate users to whom the access of the data is permitted by the data owner. For this purpose, the concept is represented in figure 4 where user1 is the data owner, user2 is the one with whom user1 has shared the data, and user3 is the one to whom user2 wants to forward the data. In the presented case, when the

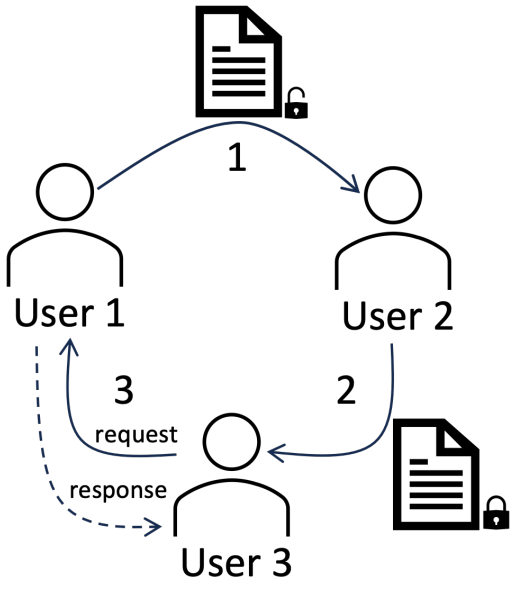


Fig. 4: Consensual Data Sharing

read authorized user2 for the data owned by user1 tried to forward the data to another user permission control mechanism

that is implemented at the levels of the main chain and side chain for user1 ($\mathfrak{SC}_{O_i'}$). The consensual sharing mechanism is presented in algorithm 1 which takes $\mathbb{data}$ as input s.t. $\mathbb{data}$ always belongs to not null data contributor. The outcome of this algorithm is the surety that only the permitted data is shared with others.

The algorithm enables identifying and establishing consensual sharing along with the mechanism to deal with unauthorized/ flagged data access requests through logging of such access attempts in $\mathfrak{MC}$ as $\mathfrak{MC}(alert(R_{\mathbb{data}_j}))$. The ownership rights of data elements are checked, and if the user trying to forward the data is either the owner or the owner (O_i') permits the sharing by giving consent in the form of $O_i' = agree$ for $\mathbb{data}_j$.

Algorithm 1 Multichain Consensual Data Sharing Algorithm

Require: $\mathbb{data} \in \sum_{i=1}^{n} O_i' \neq null$
Ensure: $S_{\mathbb{data}} \in (7 \cap \mathfrak{SC}_{sup} \supseteq 8)$
1: $R_{\mathbb{data}_j} \rightarrow \mathbb{data}_j \subset \{O_i'\}_{\mathbb{data}}$
2: **while** $R_{\mathbb{data}_j} \neq \phi \ \& R_{\mathbb{data}_j} \notin \mathfrak{MC}(alert(R_{\mathbb{data}_j}))$ **do**
3: **if** $S_{\mathbb{data}_j} = O_i'$ **then**
4: **set:** $S_{\mathbb{data}_j}(consent) \rightarrow R_{\mathbb{data}_j}$
5: $Append : S_{\mathbb{data}_j}(consent) \in \mathfrak{MC}$
6: $Append : S_{\mathbb{data}_j}(consent) \in \mathfrak{SC}_{O_i'}$
7: **else if** $S_d \neq O_i'$ **then**
8: **send:** $S_{\mathbb{data}_j}(consent) \rightarrow O_i'(\mathbb{data}_j)$
9: **if** $O_i'(choice) = agree$ **then**
10: **set:** $S_{\mathbb{data}_j}(consent) \rightarrow R_{\mathbb{data}_j}$
11: $Append : S_{\mathbb{data}_j}(consent) \in \mathfrak{MC}$
12: $Append : S_{\mathbb{data}_j}(consent) \in \mathfrak{SC}_{O_i'}$
13: **else if** $O_i'(choice) \neq agree$ **then**
14: **set:** $S_{\mathbb{data}_j}(consent) \rightarrow Deny$
15: $Alert : R_{\mathbb{data}_j} \rightarrow \mathfrak{MC}(alert(R_{\mathbb{data}_j}))$
16: **end if**
17: **end if**
18: **end while**

C. Data Removal Rights

One of the most important aspects of GDPR requirements is the right to be forgotten, which means the data contributors can remove their data from the ecosystem. This brings in another challenge as inherently blockchains make the transactions immutable. Hence, the conventional method of keeping everyone's data onto a single chain poses challenges here. Therefore in the proposed ecosystem, this problem is proposed to be solved using multichain ecosystem. As discussed in the section III, the use of multiple chains helps in achieving this functionality along with other merits. There are two forms of data, one is metadata/ access control data that resides on the $\mathfrak{MC}$ and the other form is the actual contributed data, that never go on $\mathfrak{MC}$ but stays on $\mathfrak{SC}$ of the data contributor O_i'. The access control is governed by various types of mappings 1x1, 1xM, Mx1, and MxM. Hence when a removal request is generated by O_i' for $\mathbb{data}_j$ owned by O_i', corresponding mappings in $\mathfrak{MC}$ and $\mathfrak{SC}'_{O}i$ are updated to ϕ thus removing all-access to the $\mathfrak{SC}_{O_i'}$, the same is presented in algorithm 1. If $\mathbb{Rr}(\mathbb{data})$ is made by other than O_i' the request is marked invalid and ignored by the system.

Algorithm 2 Data Removal Request

Require: $\mathbb{Rr}(\mathbb{data})$
Ensure: $\forall O_i' \in \{O\}, R_{\mathbb{data}_j} \mapsto NULL$
1: $Get : \mathbb{Rr}(\mathbb{data})$
2: **while** $\mathbb{Rr}(\mathbb{data}) \in \{O\}$ **do**
3: **if** $\mathbb{Rr}(\mathbb{data}) = O_i' \ \&(\mathbb{data})_j \neq \phi$ **then**
4: **for** $j \leftarrow 1$ to N **do**
5: In $\mathfrak{MC}$ Set: $\mathbb{Rr}(\mathbb{data}) \rightarrow \phi$
6: In $\mathfrak{SC}_{O_i'}$ Set: $\mathbb{Rr}(\mathbb{data}) \rightarrow \phi$
7: In $\mathfrak{MC}$ Set: $\mathbb{data}_j(O_i') \rightarrow \phi$
8: **end for**
9: **else if** $\mathbb{Rr}(\mathbb{data}) \neq O_i'$ **then**
10: invalid request
11: **end if**
12: **end while**

V. Evaluation and Validations

The proposed work is evaluated for its effectiveness and feasibility through theatrical and experimental techniques discussed in this section.

Theoretical analysis of privacy and complaint readiness: The proposed framework is capable of ensuring privacy, integrity, and data ownership rights in a transparent and distributed manner. Privacy is ensured by not storing any personal information directly or indirectly leading to user profiling. Further, the data integrity is ensured using, two stages of data integrity checks, i.e. mainchain, and sidechain.

Experimental Evaluation: The proposed model components are implemented through different implementation mechanisms for performance validations which are discussed for performance as follows.

Integrity Enforced Scripting: The scripts for common mobile operating systems have been implemented to translate the logic presented in the proposed scheme section. A snippet of the script is presented in figure 5.

Mainchain and Sidechain Contracts: Further, the proposed mechanisms of the mainchain and sidechain smart contracts are implemented, and their performance metrics in terms of gas costs are presented in Table III. Moreover, the findings of various proposed modules are compared in terms of functional

TABLE III: Computational Cost analysis of functions in mainchain and sidechain

	Cost(eth)	Time(ms)
MC Contract	0.192	4364
SC Contract	0.153	3813
Integrity Check	0.0972	5034
Right Sharing	0.2147	4351
Removal Request	0.4132	7043

cost for scalability testing with a similar single-chain implementation of the same. The results are presented in figure 6 which shows that due to better pipelining of processes in a multichain ecosystem, scalability is more favored.

```
private fun saveParametersToFile(parameters: String) {
    val fileName = "radio_parameters.txt"
    val file = File(filesDir, fileName)

    try {
        val fos = FileOutputStream(file)
        fos.write(parameters.toByteArray())
        fos.close()
        showToast("Parameters saved to file: ${file.absolutePath}")
    } catch (e: Exception) {
        showToast("Error saving parameters to file: ${e.message}")
    }
}

private fun calculateHash(data: String, key: String): String {
    try {
        val messageDigest = MessageDigest.getInstance("SHA-256")
        val input = (data + key).toByteArray()
        val hash = messageDigest.digest(input)
        val hexString = StringBuilder()

        for (byte in hash) {
            val hex = Integer.toHexString(0xFF and byte.toInt())
            if (hex.length == 1) {
                hexString.append('0')
            }
            hexString.append(hex)
        }

        return hexString.toString()
    } catch (e: NoSuchAlgorithmException) {
        showToast("Error calculating hash: ${e.message}")
        throw RuntimeException(e)
    }
}
```

Fig. 5: Integrity Enforced Mobile Equipment Script Snippet

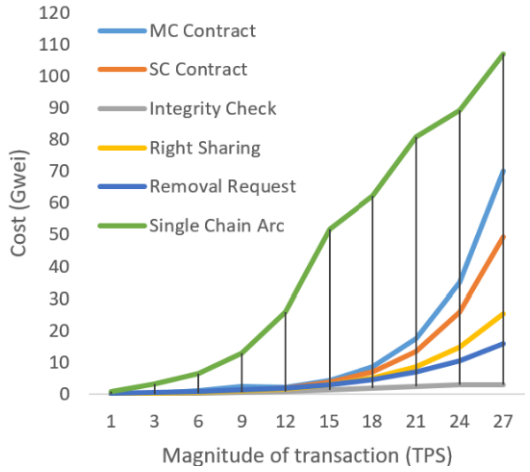


Fig. 6: Functional Cost Analysis

VI. Conclusion

The proposed mechanism is for building better user trust in the crowdsourcing ecosystems by enabling users with more control over what they contribute. In the current stage of the work, the ecosystem has been designed and its functionalities have been focused on, ensuring the data contributed by the user equipment is not manually altered. Further, the user has been provided with the power to control who they share their data with along with logging for unauthorized attempts for data access. Moreover, the mechanism to exercise the right to removal of information is explored using the multichain mechanism. The various mechanisms proposed are implemented and validated for their worthiness and results suggest their competitiveness. In the future, the work is to be extended to a full-scale working model and test and tweak the performance of the same.

References

[1] D. Marikyan, J. Llanos, M. Barati, G. Aujla, Y. Li, K. Adu-Duodu, S. Tahir, O. Rana, S. Papagiannidis, R. Ranjan *et al.*, "Privacy & cloud services: are we there yet?" in *2021 IEEE International Conference on Service-Oriented System Engineering (SOSE)*. IEEE, 2021, pp. 11–19.

[2] M. Barati, G. S. Aujla, J. T. Llanos, K. A. Duodu, O. F. Rana, M. Carr, and R. Ranjan, "Privacy-aware cloud auditing for gdpr compliance verification in online healthcare," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4808–4819, 2022.

[3] [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

[4] G. S. Aujla, M. Barati, O. Rana, S. Dustdar, A. Noor, J. T. Llanos, M. Carr, D. Marikyan, S. Papagiannidis, and R. Ranjan, "Com-pace: Compliance-aware cloud application engineering using blockchain," *IEEE Internet Computing*, vol. 24, no. 5, pp. 45–53, 2020.

[5] H. Ahmad and G. S. Aujla, "Gdpr compliance verification through a user-centric blockchain approach in multi-cloud environment," *Computers and Electrical Engineering*, vol. 109, p. 108747, 2023.

[6] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edge-envisioned iot-based healthcare monitoring," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 491–499, 2020.

[7] Y. Lu, Q. Tang, and G. Wang, "Zebralancer: Private and anonymous crowdsourcing system atop open blockchain," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, 2018, pp. 853–865.

[8] S. Han, Z. Xu, Y. Zeng, and L. Chen, "Fluid: A blockchain based framework for crowdsourcing," in *Proceedings of the 2019 International Conference on Management of Data*, ser. SIGMOD '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 1921–1924. [Online]. Available: https://doi.org/10.1145/3299869.3320238

[9] H. Wu, B. Düdder, L. Wang, S. Sun, and G. Xue, "Blockchain-based reliable and privacy-aware crowdsourcing with truth and fairness assurance," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3586–3598, 2021.

[10] Z. Sun, Y. Wang, Z. Cai, T. Liu, X. Tong, and N. Jiang, "A two-stage privacy protection mechanism based on blockchain in mobile crowdsourcing," *International Journal of Intelligent Systems*, vol. 36, no. 5, pp. 2058–2080, 2021.

[11] D. Sheng, M. Xiao, A. Liu, X. Zou, B. An, and S. Zhang, "Cpchain: A copyright-preserving crowdsourcing data trading framework based on blockchain," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, 2020, pp. 1–9.

[12] L. Tan, H. Xiao, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchain-empowered crowdsourcing system for 5g-enabled smart cities," *Computer Standards & Interfaces*, vol. 76, p. 103517, 2021.

[13] D. Feng, L. Zhang, S. Zhang, Q. Wu, and X. Xia, "Blockchain-based secure crowdsourcing in wireless iot," *Journal of Communications and Information Networks*, vol. 7, no. 1, pp. 23–36, 2022.

[14] B. Wang, Y. Yuan, B. Li, C. Dai, Y. Wu, and W. Zheng, "Qaic: Quality-assured image crowdsourcing via blockchain and deep learning," in *2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 2023, pp. 648–653.

[15] A. Ismailisufi, T. Popović, N. Gligorić, S. Radonjic, and S. Šandi, "A private blockchain implementation using multichain open source platform," in *2020 24th International Conference on Information Technology (IT)*, 2020, pp. 1–4.

[16] M. T. Oliveira, G. R. Carrara, N. C. Fernandes, C. V. N. Albuquerque, R. C. Carrano, D. S. V. Medeiros, and D. M. F. Mattos, "Towards a performance evaluation of private blockchain frameworks using a realistic workload," in *2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 2019, pp. 180–187.

[17] C. Lin, D. He, S. Zeadally, N. Kumar, and K.-K. R. Choo, "Secbcs: a secure and privacy-preserving blockchain-based crowdsourcing system," *Science China Information Sciences*, vol. 63, pp. 1–14, 2020.