Handling Federated Privacy preserving Crowdsourcing platform on blockchain

Ms. Mrunal S. Mane[1], Prof. Sarika V. Bodake[2]

[1] *M.E Student, Computer Department, PVPIT, Maharashtra, India*
[2] *Head of Department & Guide, Computer Department, PVPIT, Maharashtra, India*

ABSTRACT

With the rising unemployment and scarcity of jobs, crowdsourcing has emerged as one of the most innovative and helpful uses in recent years. The crowdsourcing technique leverages the power of collaboration to complete difficult and huge projects by breaking them down into simpler tasks. A huge number of workers can successfully perform the minor jobs. However, there is an ongoing issue that has arisen as a result of the installation of these services on the internet architecture. There is a lack of confidence and dependability transmitted by both the task publisher and the employees, resulting in a decline in the number of users on this new platform. There have also been a few techniques intended to reduce this impact, but none of them have been fully successful in reaching better efficiency. As a result, this research proposes an effective strategy for the objective of a trust-free crowdsourcing methodology. The AES encryption system and smart contract technology are combined with Pearson Correlation and Decision Tree on a distributed blockchain architecture in the described solution. According to the experimental results, the proposed approach successfully delivers the intended objective by effective and accurate deployment of AES and the Smart Contract methodologies.

Keyword: - *Advanced Encryption Standard, Blockchain Framework, Smart Contracts, Pearson Correlation and, Decision Tree.*

1. INTRODUCTION

Due to its tremendous efficiency crowdsourcing has progressively become an essential approach to manage complicated issues and finish huge projects by combining crowd power and machine learning. Large-scale translation, information collection, and even more advanced computer systems, such as picture annotation, are only a few examples. The crowdsourcing method is highly useful for finishing a tough work by enlisting the help of a large number of people to do little portions of the task at a time. As a result, the highly difficult work is broken down into a series of smaller activities that can be readily done by an average person. As a result, when crowdsourcing techniques were first presented, they acquired a lot of attention.

Outsourcing the work relieves the organization of its burden and leads to a better strategy, which reduces the strain substantially. This results in a better experience for both the employee and the company, further increasing efficiency. However, the crowdsourcing technique has always been plagued by a lack of effective and secure implementation.

The majority of the early adoptions and initiatives were aimed at getting a large number of people to utilize this platform. This was described as a result of the necessity to increase the approach's exposure and make it easier for businesses to select the best worker for their duties. This has resulted in an overpopulation of people, many of whom

have malevolent intentions toward the job that is being done. Because of the many security flaws exploited by users, the prevalence of these techniques has been extremely concentrated.

The task assigned to the worker is a small portion of a larger and more sensitive activity performed by a certain organization. It may include extremely sensitive information about the company, which might be troublesome if it is engaged in a security breach or leak. This may be a troublesome situation that, if managed improperly, might end in devastating consequences. This is a dilemma for the task providers since their information may be in jeopardy, putting their own and the company's confidential material at jeopardy. As a result, the data that is transferred to the worker must be protected.

These events have resulted in a loss of confidence among those participating in the crowdsourcing process. As a result, the number of people successfully participating on this medium has steadily decreased. The worker's aspect of the trust issue is also present, since there have been occasions where work has been completed on time and sent to the task provider. Following the submission, the task provider defaults to pay the agreed-upon compensation for a job well done. This causes contempt in the worker, which results in a decrease in the worker's approach's dependability.

As a result, the suggested technique was developed, which has shown to be effective in establishing a trustless and dependable foundation that holds all of the approach's players accountable. The integration of the blockchain framework provides the security. This enables for tamper-proof protection, which can help secure data. The smart contract technique enhances dependability and achieves effective responsibility from both parties involved. Both the worker and the job providers are held accountable under the reward and penalty system. The methodology has been thoroughly discussed in the following sections of this research article.

The subsequent section 2 below outlines the related work that has been analyzed, whereas section 3 details the various steps performed by the proposed system. Section 4 deals with the experimental outcomes and finally the section 5 provides the concluding statements and the future research directions.

2. LITERATURE SURVEY

Liping Gao [1] introduce TSWCrowd, a completely distributed job discovery worker crowd-sourcing solution that combines crowdsourcing and blockchain technology. TSWCrowd, in compared to conventional organised crowdsourcing platforms, focuses on two issues: efficient crowdsourcing delivery and the promise of job benefits. Switch off-chain operations to on-chain operations using blockchain technology to assure transaction accountability and fairness. TSWCrowd permits requesters to pay in advance and leverages non-tamperable blockchain data to ensure that employees who complete jobs and provide responses receive straightforward recompense, increasing workers' enthusiasm for participating in the scheme. When compared to the off-chain VCG method, staff travel time is greatly reduced, indicating that TSW is lower and more reasonable. Workers' overall remuneration in the TSWCrowd model is higher than in the on-chain ABCrowd model, indicating that TSWCrowd is more sensitive of their requirements.

Hui Lin [2] discusses that integrating Blockchain, DRL, and spatial crowdsourcing technologies, a Deep Reinforcement Learning and Blockchain-based Spatial Crowdsourcing Framework (DB-SCS) for SDN-IoV implementations can be designed. The geographical crowdsourcing network, blockchain layer, and DRL layer are the three layers of the DB-SCS scheme. The user credit management procedure is handled by the spatial crowdsourcing layer, which is in charge of handling users and activities. DB-SCS suggests a multi-blockchains-based hierarchical task classification and management strategy, as well as a DRL-based job allocation system, to maintain task secrecy during the work allocation and release cycles. Furthermore, for various SDN-IoV scenarios, a DRL-based blockchain performance optimization framework is designed to strike a balance between privacy protection and device performance. Simulation results show that the DB-SCS will maintain privacy and stability in the face of internal Sybil and collusion attacks.

Chen Zhang [3] describes PFcrowd, a federated and privacy-preserving crowdsourcing system. It allows brokers to offer proposals and employees to take on work using blockchain technology via various crowdsourcing platforms. The authors create an encrypted task-worker matching without involving any third-party jurisdiction. Through many brokers' on-chain task indexes, it will promote approved task-worker matching. On Ethereum, the PFcrowd platform

is launched and tested. To demonstrate security weaknesses, the authors conduct a detailed vulnerability review. PFcrowd's utility is demonstrated by extensive evaluations of real-world datasets.

Liang Tan [4] explains the Crowd Chain framework, which is a shared trustworthy service platform for crowdsourcing programmes that is based on blockchain technologies. The authors abolished the third-party payment entity PAT and incorporated blockchain, which is represented by BC, based on the classic traditional crowdsourcing architecture. In the service mechanism, there is a lack of confidence centers or payment center institutions. Requesters, personnel, and the crowdsourcing network may all review the data information generated in the framework, making the entire crowdsourcing service process visible and transparent. Furthermore, the payment of the service charge, the provision of the reward, and the settlement of the refund are all done within the blockchain, which is safer, faster, and easier than utilizing third-party central payment facilities.

Vikas Hassija [5] narrates a traffic jam probability estimation, a crowdsourcing technique based on blockchain. Users can receive tokens as part of the blockchain network by trading real-time traffic data, which consumers can then utilize to acquire traffic information from the network The authors utilized an LSTM neural network with the output from a feed-forward ANN trained on statistical information for live data-based traffic jam probability estimation. A compensation mechanism is also presented to increase customer desire to participate in the crowdsourcing approach for predicting traffic jam severity. According to the findings, the given model receives a higher level of consumer participation as a result of the additional incentive, resulting in highly trustworthy outcomes.

Maha Kadadha [6] expresses that ABCrowd is a fully distributed crowdsourcing system that incorporates auction processes using blockchain. The described ABCrowd crowdsourcing tool takes advantage of the Ethereum blockchain as well as open crowdsourcing. The ABCrowd platform is built exclusively on Ethereum and utilises smart contracts to overcome the challenges of centralised and off-chain execution. As a result, personnel and requesters have faith in the implementation system ABCrowd addresses two major issues: blockchain-based trust and worker authenticity via the R-SMB honest auction mechanism. Upon contrasting the on-Chain R-SMB mechanism to the streamlined off-Chain VCG mechanism, it's clear that R-SMB comes close to VCG in terms of job delegation, while surpassing VCG in based on requesters' overall cost and workers travelled distance.

Shuai Wang [7] presented a unique decentralized knowledge graph building solution based on blockchain powered smart contracts, which use the knowledge graph as a deep recommender strategy, with case studies demonstrating the system's efficiency. Three advantages of the recommended technique are as follows: First, it uses the wisdom of crowds to maintain a strong balance between the fullness and accuracy of the information graph; second, the decentralized design process is extremely trustworthy because all results are recorded on the blockchain. This method is transparent, highly secure, and resilient. The most essential benefit is that, as a result of the on-chain/off-chain feedback, the information graph is constantly developing and updating.

Yifan Tian [8] envisioned a decentralized blockchain-based framework for reliable and accurate truth detection. The application, blockchain, and storage layers make up the framework as a whole. Due to the limited on-chain storage capacity of blockchain, the authors segregated the logic plane, which consists of the blockchain and application layers, from the data plane, or storage layer, in the architecture. The data's accompanying pointers are submitted to the blockchain, while the remainder of the data is saved in the storage layer. Despite the massive motivation for truth discovery implementations, the proposed system uses smart contracts to permit the requester to get an accurately computed truth discovery outcome without requiring to undertake time-consuming verification. Meanwhile, the authors built a smart contract with a very effective confidentiality method based on perturbation, resulting in a strong privacy guarantee for each worker's information. Because of its modular nature, the provided system frequently eliminates the risk of a single point of failure.

Nitin Sukhija [9] in this publication for data crowdsourcing, developed a blockchain-based open information access and control system. The structure described is made up of three layers: user, blockchain, and data. The user layer is an interactive graphical user interface built using the React JavaScript Library (GUI). By sending out a web form with checkbox selections and an input box for their email address, NERSC or external users may pick the operational datasets they want to acquire. The blockchain layer is powered by two main frameworks: Hyperledger Fabric and Hyperledger Composer. Business Networks are created by combining the two tools, with the composer generating them and the fabric operating them locally. The datasheet is made up of the databases that will be

crowdsourced using OMNI. Elasticsearch, a resilient and concurrent time-series database, is used to enable this architecture, which comprises a single location for storing heterogeneous datasets. The architecture provided here provides researchers with immutable, straightforward access to organizational data and aids in the authentication, confidentiality, and visibility of datasets while releasing information to the public in a controlled way.

Konrad Wrona [10] narrates that as part of civil-military collaboration, a blockchain-based encrypted linkage of metadata to sensor data obtained in smart environments was demonstrated. For the given method, Hyperledger Fabric has been recommended as a possible deployment platform. Hyperledger Fabric is among the most comprehensive and widely used frameworks for developing blockchain-based applications. STANAG 4774 and 4778 were also developed by NATO to guarantee that material was categorized uniformly. The authors presented a high-level architecture based on STANAG 4774 and 4778 codebases for a metadata linking method. The sensor data and information are stored on a Hyperledger Fabric.

Chi Harold Liu [11] presented a combined IIoT architecture that blends energy-efficient information gathering with secure data exchange across MTs or Mobile Terminals enabled by blockchain and DRL. A decentralized DRL-based solution was developed for each MT to shift a data collecting site while maintaining the excessive data gathering ratio and regional equity overtime. When MTs exchange data, Ethereum is used to preserve the confidentiality and dependability, allowing Ethereum to simply manage a tamper-proof record maintained by all collaborating MTs without the requirement for a trusted third-party central authority. The results of the experiments revealed that, when contrasted to a traditional database management and sharing system based on the MySQL database, the proposed strategy can provide better information sharing security, durability, and resilience to harmful assaults such as DoS, DDoS, and so on.

Jun Zou [12] presents a complete blockchain-based strategy to service accountability standards that addresses both functional and non-functional aspects. In combination with incentivized steps, the authors proposed a Proof-of-Trust consensus protocol that incorporates a trust element to fulfil realistic needs in the service sector, that is, to address suspicious behaviors that frequently appear in a visible, public service network. The system employs a unique approach that divides transaction validation and block preservation into two categories. This type of organization would aid in balancing centralization and decentralization, as well as stability and accountability.

Yuan Lu [13] provides a fundamental game theory viewpoint to an expression of the intrinsic flaws of public blockchains, permitting the chain to “audit” the operation of a wide range of computationally demanding applications. The architecture provided here proposes a simple incentive structure that allows the blockchain to crowdsource the development of a wide range of sophisticated applications while preventing any misleading computing capacity. The procedure provided here works in situations when there is no reliable third-party involvement Furthermore, the protocol may facilitate any potential coalition, where n denotes the entire population of service providers not simply those who are not colluding as n-1.

3. PROPOSED METHODOLOGY

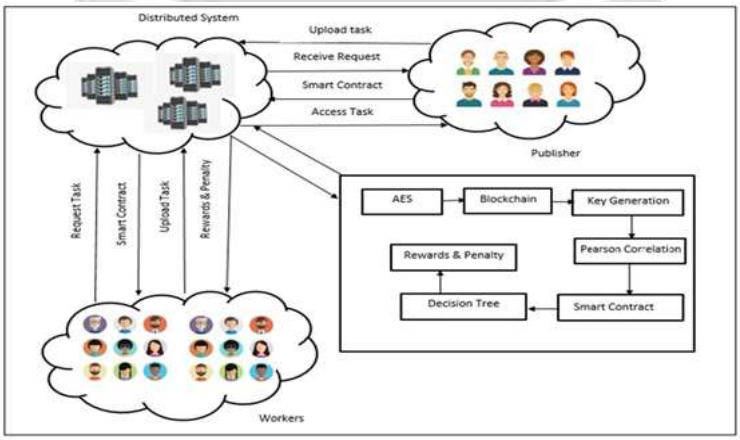

Fig -1: System overview Diagram

The proposed methodology for attaining effective crowdsourcing derived through the deployment of distributed blockchain platform is illustrated in Fig. 1 above. The methodology has been explained step by step below.

Step 1: Task Upload and AES – The presented technique for the crowdsourcing implementation is initiated which requires a task to be published. The task publisher is concerned with the publishing of the task, therefore, the respective task to be realized is posted on the platform. For enabling robust security for the task being uploaded on the system, an encryption mechanism called AES is being deployed. The task is then encrypted using the AES encryption mechanism and the key is needed to be generated. For the key generation of the encrypted data, the MD5 hashing algorithm is being utilized. The MD5 generates a hash key which is further processed by eliminating the characters and achieving a 7 character key. This key constitutes an integral part of the blockchain formation and storage of this data on the distributed server which is depicted in the subsequent step. The algorithm 1 describes the key generation procedure below.

ALGORITHM 1: Signature Key Generation

//Input : Task List T_L
//Output: Signature Key KEY
Function: keyGeneration(T_L)
1: Start
2: con = " ", KEY= ""
3: for i=0 to size of T_L
4: s = s + $T_{L\,[i]}$
5: end for
6: $MD5_K$=MD5(s)
7: R= $MD5_K$ SIZE MOD 7
8: for j=0 to KEY Length < 7
9: j=j+(R+1)
10: if (j< $MD5_K$ length)
11: KEY=KEY+ $MD5_{K\,[j]}$
12: $MD5_K$ = $MD5_K$ >> 1
13: else
14: j=0
15: end for
16: return KEY
17: Stop

Step 2: Blockchain Formation – This technique of blockchain formation uses the task submitted by the task publisher in secure manner as an input. The MD5 hashing algorithm key that was created in the preceding stage will be utilized to create the block head for the relevant block in the blockchain. On that basis, a block comprising encrypted data and its associated hash key are created, which is kept in the head.

The next tasks that are going to be uploaded on the need to be subjected to the same procedure and added to the blockchain. As a result, all additional files or data posted to the site must be linked to the current blockchain. Each subsequent file is merged with the preceding block's cryptographic hash key, and the hash key for the current block is computed. This chain links the two blocks together. In order to create the block's head, a new hash key must be produced. Each file that is uploaded for that job goes through the same process. The terminal key, which is the final key of the final block, is saved in the database for subsequent integrity checks to be performed. The algorithm 2 describes the blockchain formation process below.

ALGORITHM 2: Blockchain Formation

//Input : Task list T_L
//Output: Terminal Key T_{KEY}
blockchainFormation(T_L)
1: Start

2: T_{KEY} =" "
3: for i=0 to size of T_L
4: P= $T_{L\,[i]}$
5: T= getFileContent(P)
6: T = T + T_{KEY}
7: H_K=MD5 (T)
8: TRM_{KEY} = signatureKey (H_K)
9: end for
10: return T_{KEY}
11: Stop

Step 3: Pearson Correlation – The correlation between two different and continuous entities can be effectively evaluated through the use of Pearson Correlation. The Pearson correlation is being utilized to detect any penalties or rewards being issued to the workers through the evaluation of their profile and their previous tasks. The performance of the worker needs to be extracted for the task publisher as the owner of the task needs to understand the capability of the worker before assigning the task. The methodology being elaborated has deployed an effective reward and penalty strategy for the purpose of enabling a better experience for both the owner and the worker. The assessment procedure is enacted to ensure that the worker is a reliable worker or not. The determination of the Pearson correlation is performed through the equation 1 given below.

$$r = \frac{\sum xy - \frac{\sum x \sum y}{n}}{\sqrt{(x^2 - \frac{\sum x^2}{n})}\sqrt{(y^2 - \frac{\sum y^2}{n})}} \quad \text{_____ (1)}$$

Where

x is the worker completing a number of tasks

y is the evaluation of the work through rewards and penalties

n is the size of the array

r= correlation coefficient

The measurement of the correlation coefficient from the equation above, results in a value between -1 and 1. The coefficient values that are closer to +1 are indicative of an exceptional performance from the worker. The coefficient closer to 1 dictates a larger concentration of rewards and a value nearer to -1 indicates a larger number of penalties. This is useful for segregating the worker and allows the owner or task publisher to select the best possible worker for the task allowing better work ethic and quality results.

Step 4: Smart Contract – Once the owner is satisfied with the worker and the Pearson correlation coefficient is positive, then the owner selects the worker. This worker needs the task to start their work, therefore, the task details need to be shared. For this purpose, the smart contract is initiated, this is due to the fact that the data for the task is present in the form of a blockchain. This smart contract when implemented, takes both the owner profile and the worker profile to generate individual keys pertaining to their respective profile attributes.

The smart contract is designed in a way to facilitate the secure sharing of the information that would be robust and prevent any manhandling of the data being shared. Therefore, these Owner Key and the Worker key are combined to generate the Smart Contract key. This key is then used to accurately secure the data being shared. The implementation of the smart contract key cements the reliability of the data, as the data cannot be shared with anyone else other than the owner and the specified worker. This is the part where the approach is provided with maximum reliability and accountability from both the parties involved. Thus, the smart contract can be considered as the most integral part of this methodology pertaining to the security and reliability aspect.

Step 5: Decision Tree – The Decision Tree approach is being implemented in this research to enable the effective realization of the classification of the correlation coefficients. The Pearson Correlation values are provided as an input to this step of the approach to segregate the workers based on their effectiveness. The worker when assigned a

task, is provided with a time frame within which the worker needs to submit the work. This time frame is then utilized to provide the worker with the rewards or a penalty. If the worker submits the completed task on time and within the time frame, a reward is provide, whereas if the worker does not submit a completed task or utilizes more time to complete the task than the allotted time, they are given a penalty.

This allotment of reward and penalty to the worker is an essential task that needs to be effectively deployed to understand the worker quality and provide the owners with a better outcome. The Decision Tree implements the if-then rules to perform the classification and provide label for the reward or penalty. The reward and penalty strategy provides a robust and reliable way for the implementation of the crowdsourcing methodology that enhances it considerably.

4. RESULTS AND DISCUSSIONS

The presented methodology for the purpose of enhancing the crowdsourcing approach through the deployment of the distributed blockchain platform. The methodology has been designed using the Java programming language and has been realized on a deployment machine consisting of 500 GB storage, 6 GB RAM and an Intel Core i5 processor. The MySQL database is being used for the management and organization of the data.

The performance metrics of proposed system needs to be evaluated to determine the accuracy of the implemented modules in this procedure. There are various modules in this methodology, but the main concentration is security and reliability that is being improved in this methodology. Therefore, the encryption modules are being tested for their accuracy in the section given below.

4.1 Character assignment for Encryption Comparison

The presented technique has been evaluated by a number of different assessments which have been performed to determine the performance of encryption and decryption achieved by the AES module being deployed in the prescribed approach.

In-depth analysis is performed to derive the performance of cryptography employing the AES algorithm undertaken in this technique. For this measurement, the number of characters being used for AES encryption is contrasted to the value achieved in [14]. The relationship of the encryption techniques has been carefully investigated and is presented in table 1 below.

Table -1: Characters utilized for Encryption (AES v/s RCC)

S no.	No of Characters	AES	RCC [14]
1	0	0	0
2	1000	51	42
3	2000	57	51
4	3000	59	48
5	4000	60	55
6	5000	63	52

The analysis suggests that AES encryption needs a much greater number of characters for encryption and decryption operations. When contrasted to the RCC encryption method specified in [14]. The resultant outcomes from the table are plotted in figure 2 below for easier representation.

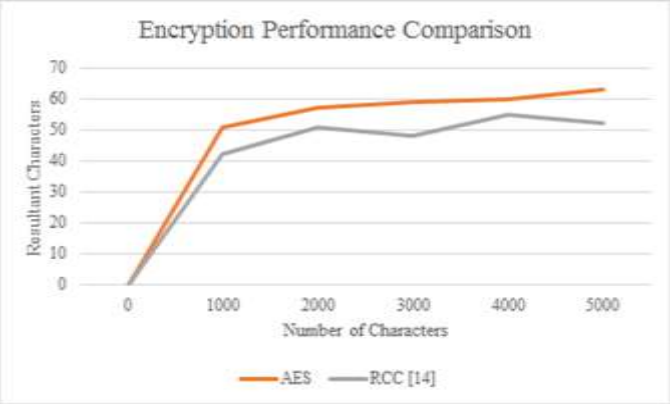

Fig -2: AES v/s RCC character count comparison

Figure 2 illustrates the benefit of the encryption technique provided in the proposed technique over the RCC encryption strategy reported in [14]. The rise in sophistication of the method may be ascribed to this feature, since increasing the amount of characters in the AES encryption procedure significantly increases confidentiality. The enhanced security of the encryption makes it tougher to penetrate, which further discourages any intrusions on the system.

4.2 Encryption and Decryption Time performance

The presented approach has been further evaluated for its cryptography performance by determining the time taken for the encryption and decryption process. This is a highly useful metric as it allows for a much better understanding of the time complexity in this implementation. The lower amount of time taken can considerably decrease the overall execution duration of the proposed system. This is an effective technique for the reduction in the time complexity that can be seen as the most effective and useful mechanism that is quantified to determine the effective performance of the technique. Encryption and decryption times of the provided system have been evaluated and are summarized in Table 2 below.

Table 2: Encryption and Decryption time performance

Number of Characters	Encryption Time in Milliseconds	Decryption Time in Milliseconds
16	2	2
1798	15	16
2689	29	32
3014	46	50
4679	52	51
5898	61	60
6617	66	61
8163	78	88
8994	79	89
9961	88	93

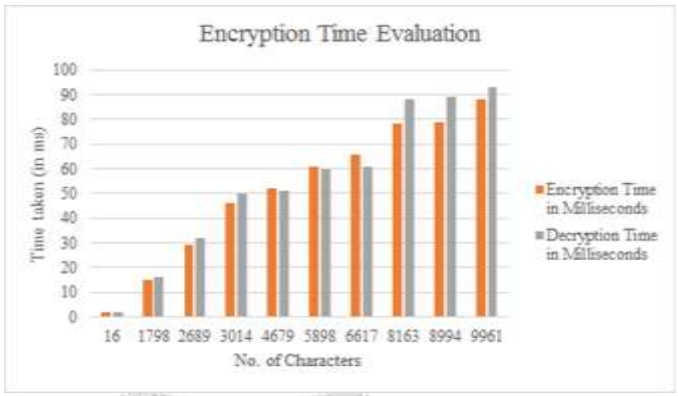

Fig -3: Encryption and Decryption Time

A glance at Figure 3 above demonstrates how encryption and decryption times are not directly related to the amount of characters. After completing the evaluation, it was determined that the encryption and decryption technique had been successfully executed with no anomalies identified.

5. CONCLUSION AND FUTURE SCOPE

A trustless crowdsourcing technique is outlined in this research paper. For the task to be published by the task publisher, an effective system has been created that allows a lot of workers to successfully do these jobs. On upload, tasks are successfully encrypted using advanced encryption standard or AES, and then a key is produced using MD5. As the block consists of the task that is shared, this key is utilized to produce the blockchain head. After that, the worker receives the job through a smart contract key. If the worker does not finish and upload the job within a certain time frame, a penalty will be imposed. The Pearson correlation is then used to determine the worker's trustworthiness based on their prior duties, rewards, and punishments. As a result of the use of decision trees, the reward and penalty system has the ability to be disseminated with more accuracy, therefore increasing the overall dependability of crowd sourcing.

The creation of an effective web application for simplicity of deployment and usage in a real-time environment can be one of the future areas of research for enhancing this technique.

6. REFERENCES

[1]. Liping Gao, Tian Cheng, and Li Gao, “TSWCrowd: A Decentralized Task-Select-Worker Framework on Blockchain for Spatial Crowdsourcing", IEEE Access (Volume: 8), 07 December 2020.

[2]. Hui Lin, Sahil Garg, Jia Hu, Georges Kaddoum, Min Peng and M. Shamim Hossain, “Blockchain and Deep Reinforcement Learning Empowered Spatial Crowdsourcing in Software-Defined Internet of Vehicles", IEEE Transactions on Intelligent Transportation Systems (Early Access), 15 October 2020.

[3]. Chen Zhang, Yu Guo, Hongwei Du, and Xiaohua Jia, “PFcrowd: Privacy-Preserving and Federated Crowdsourcing Framework by Using Blockchain", 2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS), 06 October 2020.

[4]. Liang Tan, Huan Xiao, Xinglin Shang, Yong Wang, Feng Ding, and Wenjuan Li, “A Blockchain-based Trusted Service Mechanism for Crowdsourcing System", 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), 30 June 2020.

[5]. Vikas Hassija, Vatsal Gupta, Sahil Garg, and Vinay Chamola, “Traffic Jam Probability Estimation Based on Blockchain and Deep Neural Networks”, IEEE Transactions on Intelligent Transportation Systems (Early Access), 03 June 2020.

[6]. Maha Kadadha, Rabeb Mizouni, Shakti Singh, Hadi Otrok and Anis Ouali, “ABCrowd An Auction Mechanism on Blockchain for Spatial Crowdsourcing”, IEEE Access (Volume: 8), 10 January 2020.

[7]. Shuai Wang, Chenchen Huang, Juanjuan Li, Yong Yuan, and Fei-Yue Wang, "Decentralized Construction of Knowledge Graphs for Deep Recommender Systems Based on Blockchain-Powered Smart Contracts", IEEE Access (Volume: 7), 19 September 2019.

[8]. Yifan Tian, Jiawei Yuan and Houbing Song, "Secure and Reliable Decentralized Truth Discovery using Blockchain", 2019 IEEE Conference on Communications and Network Security (CNS): Workshops: DLoT: 2nd International Workshop on Distributed Ledger of Things, 2019.

[9]. Nitin Sukhija, Elizabeth Bautista, Moon Moore, and John-George Sample, "Employing Blockchain Technology for Decentralized Crowdsourced Data Access and Management", 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 09 April 2020.

[10]. Konrad Wrona and Michal Jarosz, "Use of Blockchains for Secure Binding of Metadata in Military Applications of IoT", 2019 IEEE 5th World Forum on the Internet of Things (WF-IoT), 22 July 2019.

[11]. Chi Harold Liu, Qiuxia Lin, and Shilin Wen, "Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning", IEEE Transactions on Industrial Informatics (Volume: 15, Issue: 6, June 2019), 28 December 2018.

[12]. Jun Zou, Bin Ye, Lie Qu, Yan Wang, Mehmet A. Orgun and Lei Li, "A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services", IEEE Transactions on Services Computing (Volume: 12, Issue: 3, May-June 1 2019), 06 April 2018.

[13]. Yuan Lu, Qiang Tang, and Guiling Wang, "On Enabling Machine Learning Tasks atop Public Blockchains: A Crowdsourcing Approach", 2018 IEEE International Conference on Data Mining Workshops (ICDMW), 11 February 2019.

[14]. Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi, "Reverse Circle Cipher for Personal and Network Security", 2013 International Conference on Information Communication and Embedded Systems (ICICES), 29 April 2013.