International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Maintaining Decentralized Framework for Crowdsourcing using Blockchain

Prasad B .Suryakar and Virendra V. Bagade

Computer Engineering PICT, Pune, India

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Unemployment has been on a steady rise in major countries all across the world. There is also a growing need for small tasks that need to be completed in an organization at the same time. Therefore, the Crowdsourcing paradigm is being widely used nowadays for a wide variety of fields. This allows the organization heads to get their small tasks done without employing a large workforce. The crowdsourcing platform also offers a lot of part-time employability to a large subsection of the populous which will share the complex workload to achieve efficient task completion. The only limitation of this platform is the lack of security and the presence of malicious users that reduce the Quality of service for the workers as well as the task publishers. Therefore, for the purpose of implementing a secure crowdsourcing platform Blockchain is utilized effectively. The blockchain platform increases the security of the system and helps introduce a Reward and Penalty based scheme that introduces accountability into the system for the worker as well as the task publishers. The proposed technique utilizes Entropy Estimation through Shannon Information Gain along with Decision tree and Blockchain to implement a secure crowdsourcing paradigm.

Keywords: *Blockchain, Shannon Information Gain, Decision Tree, Data Vending.*

Introduction

Unity is a strength, this phrase has been extensively used to demonstrate the potential of a group of individuals. A significantly large group of individuals can be a force to reckon with, most of the wars in our history have demonstrated this fact. Large groups of people working as a single unit can achieve what an individual could take years to achieve, united we stand divided we fall is a very true fact, a group of determined people can achieve a task that would be impossible otherwise. This has been utilized in the corporate world, where tasks and problems are segmented and distributed to the workers that execute the task and solve the problem simultaneously.

This mentality gives rise to the Crowd Sourcing platform. The crowd intelligence platform works on the same concept, a group of individuals with average intelligence can solve a problem better than a single really intelligent person solving it. Crowd Intelligence is an innovative concept that is highly useful for the optimization of the various complex as well as computationally intensive workloads. The combined efforts of the group and their collective intelligence is a boon for this type of intensive tasks and can also reach high efficiency.

The concept of crowdsourcing revolves around the augmentation of the problem-solving ability and reducing the time taken for reaching a suitable solution. It has been analyzed that a group of individuals with average intelligence is combined can solve the problems much more efficiently and faster than employing an individual with above-average intelligence when applied in various different streams such as Cognitive Sciences, Social Psychology, and Management Science. Therefore, this can be a highly useful phenomenon that would eliminate a lot of work in a short duration while employing and benefitting a large section of people.

The main idea behind this crowdsourcing for an organization is that the collection of humans behaves and works like a single unit or an organism. All the different parts of these organisms are actually individuals that are working together towards a singular and very specific goal. The tasks are divided and interlinked between the various different individuals. The crowdsourcing platform is responsible for synchronizing the various different tasks between those individuals and coordinate the various processes between the workers. This is the main crux of the system that alleviates it and makes the whole organism more intelligent than all the intelligence of the individuals combined.

The Crowdsourcing platform is highly powerful and is being used extensively in largescale applications across various different industries. NASA has also been

utilizing crowdsourcing to segment and identifies new stars as it is highly time-consuming for the researchers to sit down and segregate the stars. Therefore, an online crowdsourced task was created for individuals from any background to help with segmentation and identification of the stars by making the users perform the task on a small patch of the space. This was a resounding success as the crowd managed to accurately segment the sky and the stars but also ended up identifying new stars too.

Therefore, it can be concluded that the collective competence of the individuals can have a large impact on even the most complex of tasks and crowd sourcing can help us achieve some significant milestones with this approach. The crowdsourcing utilizes the communication between the various entities that help function as a very intelligent organism or entity, working in unison. The crowdsourced system can trump any intelligent individual any day. This large amount of collective intelligence can be used to solve the world pressing problems that require extensive expertise.

The crowdsourcing paradigm benefits greatly by the internet platform as it provides a communication channel between those individuals partaking in the crowdsourced task. The internet already has a large number of users that can contribute significantly to the crowdsourcing paradigm, this makes the internet an important infrastructure in this approach. The synchronization between the individuals in the group can also be achieved with relative ease on the internet. This paradigm has the capabilities to combine the computational power of the computers along with the insight of a large group of individuals which works like an organic computer and achieves impressive results.

But the problem with the individuals and the organizations that provide the work and complex tasks for the purpose of crowdsourcing have a lot of trust issues. This is highly undesirable as without any kind of trust between the parties involved, there would be no interaction and the crowdsourcing platform will suffer. The organization does not trust the crowd with their data and is unwilling to share, the crowd, on the other hand, is concerned about their own welfare and their data which could be at risk while sharing. Therefore, these security concerns need to be answered if the data sharing the crowdsourcing paradigm is utilized effectively.

The Blockchain paradigm is one of the leading approaches towards safe and fair crowdsourcing and data sharing paradigm. Blockchain is a novel concept that was invented to secure documents in the early 1990s. it was largely used for the maintenance of Digital notary or securing documents with a time stamp. After a brief usage, it quickly slipped into obscurity for a large time and not much research was done on this platform for a long time. This changed drastically with the introduction of Bitcoin as a Cryptographic currency which provided an alternative to the traditional fiat currency.

Satoshi Nakamoto is the developer credited with the introduction of this cryptocurrency and pulling blockchain back from obscurity. This led to increased interest in the research community regarding the Blockchain paradigm and has led to the re-emergence of Blockchain as a suitable tamper-proof application to various different types of data. The blockchain paradigm achieves this by using the blocks for the storage of data and chaining them with the help of their hash keys. This is a very ingenious process, it starts with the creation of the first block called the genesis, this block stores its data on the block and the hash key in the head.

The next transactional data is again converted into a block and the hash key is combined with the previous blocks hash key to chain both the blocks together. this is repeated for all the data elements, with the head of each block storing the previous block's Hash key. This creates a chain of data blocks that are highly secure and decentralized. This is very useful as it can detect if there has been any tampering done on the data since any change in the data would break the blockchain at the site of tampering.

This is due to the fact that the modified block's hash key wouldn't match the hash key in the previous block leading to the rupturing of the chain and thereby guaranteeing the tamper-proof nature of the blockchain. This is why its use in the crowdsourcing paradigm is highly useful as it would provide the organization the ability to safeguard their data as well as the users would be more willing to share their own data on the platform as long as its tampering and leakage are prevented. Therefore, the application of the Blockchain paradigm for the securing of the crowdsourcing is a valuable addition.

In this paper, section 2 is dedicated for literature review of past work and Finally Section 3 concludes this paper.

Literature Review

This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors work as follows.

G. Zhuo explains that there has been an increase in the number of smartphones all over the world. Therefore, there has been a shift towards mobile crowdsourcing, as the requestor can publish a task to be crowdsourced by a number of workers that can work through the smartphones that most of the individuals have with them nowadays [1]. But there has been a hurdle in collecting and aggregating the data from various different devices which can be a formidable challenge. The authors have devised an approach towards creating a privacy-preserving set operation in big data for cloud-assisted mobile crowdsourcing techniques. The extensive experimentation on the proposed methodology has produced satisfactory results.

V. Jacynyez introduces the blockchain technology and its recent rise in popularity with the introduction of the cryptocurrency bitcoin over the last few years. The Blockchain platform allows for a decentralized, permissionless framework that is used to power the cryptocurrencies. The blockchain can be used in many different applications where a distributed computation or storage is required [2]. Therefore, the authors have devised a technique called Betfuding which allows for the integration of the blockchain network into the crowdfunding platform. The proposed application has been released for free on Github and is in the beta stage right now.

F. Buccofurri elaborates on the concept of crowd-based applications and their rising popularity. As there is a lot of private information involved in a lot of workers and the requestors of the task, there is an increased need for securing the data of the users which is a priority. Most of the time there has been an implementation of the blockchain platform for a decentralized framework that preserves the privacy of the data while transacting [3]. But the Blockchain platform works on the backbone of miners which verify and approve transactions for a fee, this fee is sometimes exorbitant and cannot be paid by a number of small businesses. Therefore, the authors have proposed an alternative to the blockchain by utilizing an online social network such as twitter. The major limitation of this approach is that the authors have no formalized their approach in an abstract way which would achieve more security.

M. Ali states that the blockchain platform has been significantly adapted to the various different cryptocurrencies lately and has been a hot topic for research recently [4]. A lot of decentralized systems have been designed using this Blockchain system and also in the paradigm of PKI and DNS. The authors have presented a global storage and naming system called the Blockstack that utilizes the blockchain platform for the purpose of securing the whole system and decentralizing it. The major drawback of this technique is that the authors have not provided protection against DDoS attacks that can be highly dangerous for their system.

K. Singi explains the various stages of an SDLC or the software Development Life cycle that is being designed according to the client's specifications. The software should be adhering to various guidelines over the whole period of development and at the time of delivery. Not complying with various guidelines while development and the usage of unlicensed software might lead to a lot of Litigations and other complications [5]. Therefore, the authors propose a framework for compliance and adherence to the guidelines through the use of the decentralized blockchain framework. This framework maintains a tamper-proof trail of activities that can be analyzed to check for any lapse in compliance. The major drawback of this technique is that the system has not been deployed in a real-world implementation.

H. Duan introduces the crowdsourcing platform that has been designed to aggregate a large number of individuals working on a single goal coherently [6]. There has been a significant increase in the number of crowdsourcing platforms over the past years as this technology has been highly useful in the segmentation of a large and complex problem into smaller and relatively simple tasks that can be done by the crowd. But there are security limitations such as the use of a centralized third party for the processing and collection of the data from the crowd. Therefore, to eliminate this security concern the authors have implemented a blockchain framework that provides a decentralized and tamper-proof network for the crowdsensing platform. The major limitation of this paper is the increased computational complexity of the system.

J. Xu elaborates on the crowd intelligence platform which has been getting implemented on a large scale recently. The crowd intelligence platform is responsible for the segmentation of a massive and complex problem into smaller sections which are then solved collectively by a large group of people [7]. But there is a problem of security of the user and their data as it is being shared with a large number of people as well as the mutual trust between the worker and the work provider. Therefore, the authors implement a reward and penalty-based scheme along with the introduction of the Blockchain framework to bolster the security as well as provide a way for the accountability of the tasks. The main drawback of this paper is the lack of real-world implementation in a mobile network.

J. Huang states that there has been an increasing amount of interest in the platform of crowdsourcing over the past few years. Most of the crowdsourcing applications that have been designed are reliant on a centralized server that is responsible for all the data collection and data processing tasks. This centralized server is a security loophole that is being a deterrent for most people to contribute to this paradigm [8]. Therefore, the authors have devised a technique for the use of a blockchain framework for a decentralized crowdsourcing application that is highly secure and tamper-proof. The limitation of this research is that the authors are still in the early stages of development and there is still a need for some work to be done.

P. Yang investigates the issues of Task allocation on mobile social networks. The traditional concept of task offloading is based on the ball and bin theory and the use of the d-choice platform. But the authors have noticed that these applications fall short of the expectations and offer a very low efficiency for the

purpose of task allocation and offloading [9]. Therefore, the author proposes a novel "friend is a treasure" technique that is abed on the Top-K algorithm that facilitates the use of mobile social contacts and provides efficient and balanced task allocation and offloading. The limitation in the paper is that authors have not taken into account the social relationships while performing the allocations.

R. Ouyang explains that there has been a lack of reliable crowdsourcing applications that are efficient and also secure at the same time. The crowdsourcing paradigm has a deficiency of algorithms that can be scalable as well as effective in discovering the truths from the noisy sources. Therefore, the authors in this paper propose a truth discovery algorithm that has the capability to work in parallel for implementation in crowdsourcing applications [10]. The proposed algorithm has been extensively tested for its performance and has produced results that are highly efficient and accurate and the algorithm has been demonstrated to be highly scalable. The major drawback of this paper is that the authors have only done the empirical evaluation of the streaming algorithm.

A. Azaria comments on the various different bureaucratic influences and regulations that have been responsible for the sluggish growth in the use of Electronic Medical Records for a long time. Therefore, the authors have presented MedRec an efficient technique for the secure sharing and management of medical records through the implementation of the Blockchain platform [11]. The system is tamperproof and can provide flexible security to the patient's data on the framework. The experimental indicate the superiority of the proposed technique in achieving a highly secure platform for medical health records. The main limitation of the proposed technique is that the authors have not asses the feasibility of this implementation.

D. Peng elaborates on the crowdsourcing platforms that have been in large scale use recently and have been growing in popularity ever since. The authors in this paper have analyzed the popular crowdsourcing applications and he comes to the conclusion that most of the systems lack an incentive mechanism to compensate the user for the resources used and their efforts. Therefore, the authors devise a system for providing the users with an incentive mechanism for the remuneration of the resources that have been utilized by the individuals for the purpose of crowdsensing [12]. The proposed system increases the Quality of Service (QoS) of the provider and also provides relief to the user. The major drawback of the proposed technique is that the authors have not analyzed the quality of sensing data from the users.

K. Yang states that the framework for mobile crowdsourcing has been getting increasingly popular over the years with a lot more organizations utilizing the crowdsourcing paradigm to solve complex tasks using powerful mobile devices and a collective human effort. The increasing use escalates the privacy and security concerns over this paradigm as most of the applications involve a centralized server for all the interactions [13]. The authors in this paper detail the various shortcomings noticed in the related researches performed on this paradigm. This paper has outlined the various concerns that plague the crowdsourcing paradigm. The major drawback of this paper is that the authors have not presented any solutions to the problems faced.

D. Dang explains that the crowdsourcing paradigm has been the emerging concept in the past few years as various businesses and organizations have been readily adopting this approach towards problem-solving. The researchers also comment that this process has also been catalyzed with the widespread use of the internet and its subsequent proliferation [14]. The authors in this paper propose the crowdsourcing platform to be implemented in businesses for the tracking of the work done by the worker and the authors have also utilized the big data framework for the purpose of improving the efficiency of the whole process. The experimental results indicate that the proposed methodology is efficient and effective. The drawback of this paper is that the authors have not considered the various factors that affect the worker's quality.

X. Zhang elaborates on the rising popularity of the crowdsourcing platform as it is highly convenient for the workers as well as the organizations. In this platform, the workers are compensated for their work done and the requestors pay for the successful completion of the task accordingly. There are also cases of individuals with malicious intent that try to influence the system with dishonest replies and accusations [15]. This type of communication results in a loss of trust in the platform and the users will decline. Therefore, safeguard against these practices the authors have implemented an approach called Keep your Promise that eliminates such negative and dishonest comments and also prevents such type of behavior on the platform. The major limitation of this paper is that the proposed technique has a higher time complexity in comparison with conventional techniques.

Proposed Methodology

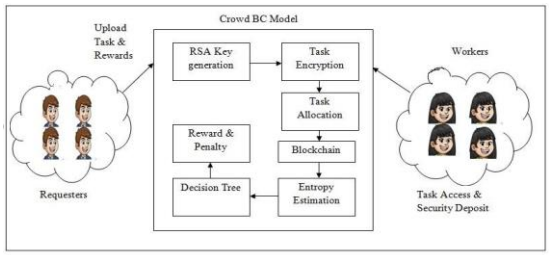

Figure 1: System Overview

The proposed methodology of the crowd sourcing using the blockchain is depicted in the above figure 1. The steps that are taken to accomplish this system is narrated in the below mentioned steps.

Step 1: Task Uploading and Reward Allocation- This is the primitive step of the proposed model where an actor called Requesters who are eagerly looking for workers to complete their task are registered into the crowd sourcing system. Once the registration is done, then these requesters are uploading the task and they are announcing the reward for the same.

Step 2: Task Encryption- This is the very important step of the proposed model where a task that is being uploaded by the requesters are need to be encrypted using the RSA cipher algorithm. As we know RSA is an asynchronous cipher algorithm which takes two keys to accomplish the encryption and decryption process. For Encryption process RSA algorithm uses the public key encryption on the other hand for the process of decryption a private key is being used.

The public key is being generated using the two natural numbers called N and E, So that public key can be given as a public (N, E). Where these two numbers are generated based on the prime numbers and the co-factors of the selected public key factors.

The private key in RSA made-up of two numbers N and D, So that private key can be given as private (N, D). Here the number D has generated based on the condition of the modulus operator to produce a unique value.

By using these private and public keys, RSA can be used for the encryption and decryption using the following two equations efficiently in the distributed paradigm of the crowdsourcing using the blockchain.

$C_D = P^E \text{ MOD } N$ _____(1)

$D_D = C_D^D \text{ MOD } N$ _____(2)

Where
C_D - Cipher Data, P- Plain data D_D- Decrypted Data

Step 3: Blockchain Formation- This is the initial step to prepare the block chain for the stored data on the servers. To create the block chain the proposed system first reads each and every task file. The task file data are then subjected to the estimate their hash values using an MD5 Hashing algorithm. Once the Hashing is done these hash keys are considered as the block head keys to form the blockchain. The final file's head key forms the complete data's integrity key. This integrity key is being used to evaluate the integrity of the data in the stored servers.

ALGORITHM 1: Blockchain formation for stored files

```
// Input: File Set Data List as DL
// Output: Integrity Key IKEY
1: Start
2: Initialize Block Head key as BHK=NULL
3: For i = 0 to size of DL
4:     File path= DL[i]
5      FCONT = getFileBytes(path)
6:     BHK = BHK +FCONT
7:        IKEY = BHK
8:    End For
9:                  return                IKEY
```

Step 4: Entropy and Decision Tree - Once the tasks are uploaded to the crowd BC system, then the workers are accepting that task through the smart contract. Once the job is finished either completely or partially then this is submitted back to the crowd BC System. On updates of task owners regarding the job completion, the crowd BC system is allocating the ranks and penalty based on the likes and dislikes given by the task owners.
Based on this the rank of the worker is being measured using the Shannon information gain equation as mentioned in
3.

$$IG = -\frac{P}{T}\log\frac{P}{T} \; -\frac{N}{T}\log\frac{N}{T} \quad \text{____(3)}$$

Where,

P= Number of Positive Likes
T= Total number of likes/dislikes.
N= T-P
IG = Information Gain of the user

Step 5: Reward and Penalty - This is the final step of the proposed model. Where reward and penalty are assigned based on the information gain values. Thereby the rank of the workers is being updated in the crowd BC system efficiently.

The whole proposed system is expressed mathematically with the below model.

Mathematical Model

1.S= { } be as system for Blockchain based Decentralized framework
2.Identify Input as T={ T_1, T_2, T_3.... T_n}
Where T= Task
S= { T_n}
3.Identify T_C and R_P as Output i.e. Task Completion , Rewards & Penalty
S= { T_n, T_C , R_P }
4.Identify Process P S= { T_n, P, T_C , R_P }
5. P= { R_{SA}, B, E_E,D_T}
Where,
R_{SA} =Rivest–Shamir–Adleman
B=Blockchain
E_E=Entropy Estimation
D_T=Decision Tree

So the Complete system for heart failure prediction can be given as
6.S = { T_n, R_{SA}, B, E_E,D_T, T_C , R_P }

Results and Discussions

The presented technique for a secure crowdsourcing paradigm has utilized the NetBeans environment for developing this technique which has been developed using Java programming language. The Development machine is powered by an Intel i5 processor equipped with 4 GB of RAM and 500 GB of storage. The data management and storage responsibilities have been handled by the MySQL database. And the propose model uses the D-Link WIFI Router for the purpose of data routing.

The proposed secure crowdsourcing platform has been analyzed for its accuracy and security through the use of intensive experimentation. The outcomes of the analysis have been elaborated below.

Character assignment for Encryption Comparison

The presented technique has been evaluated through the use of specialized tests that have been devised for the purpose of encryption and decryption performance. The RSA encryption technique has been utilized in this methodology that has been put under the hammer for the evaluation.

RSA encryption is one of the most popular encryption techniques that have been used for securing data all over the world. The RSA encryption is an asymmetrical encryption algorithm and not a symmetrical encryption algorithm. The asymmetrical algorithm utilizes two different keys one for the purpose of encryption and the other for decryption. The RSA has two keys a public key and a private key, consisting of a pair of numbers that are utilized for encryption. The public keys are distributed for encryption whereas the private keys are utilized for the purpose of decryption and are kept private.

The performance of the RSA algorithm used in this methodology for the purpose of encryption purposes has been analyzed through a set of experiments. The number of characters is the parameter utilized for the purpose of comparison of the encryption performance with the one utilized in [16]. The comparison of the encryption technique has been extensively performed and tabulated in table 1 given below.

Table 1: Number of characters utilized for encryption (RSA v/s RCC)

Experiment No	No of Characters	No of Different Characters (RSA)	No of Different Characters (RCC)
1	0	0	0
2	1000	49	45
3	2000	57	49
4	3000	75	68
5	4000	63	57
6	5000	57	50

The data described in table 1 above indicates that the RSA encryption utilizes a considerably larger number of characters for the purpose of encryption as well as decryption in comparison to the RCC encryption technique used in [16]. The tabulated values are plotted in figure 2 given below.

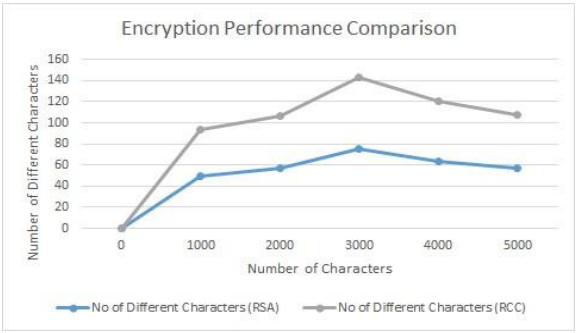

Figure 2: Plot of the number of characters utilized for encryption in RSA v/s RCC encryption techniques.

The plot in figure 2 above demonstrates the complexity of the encryption technique utilized in the proposed methodology over the RCC encryption technique explained in [16]. This is due to the fact that the RSA encryption utilizes an increased number of characters for encryption which elevates the complexity of the system which in turn increases the security considerably. The increased complexity makes the encryption difficult to decipher and ensures the security of the data that is being encrypted.

Conclusion and Future Scope

There has been a considerable increase in the unemployability in the world, specifically the developing countries. This is also corroborated with the increase in demand for temporary workers by large-scale organizations. This problem has been solved through the increasing use of online crowdsourcing platforms that have enabled a lot of convenience for the workers as well as the requestors. But this platform has been plagued with cheating and

untrustworthy practices that have led to a lot of users not opting for this platform. Therefore, to increase the security of the system and introduce a reward and penalty scheme through the use of Entropy Estimation with the use of Shannon Information Gain along with Decision tree and Blockchain decentralized Framework Future work, the proposed methodology can be implemented in remote servers. Another useful addition to this platform is to implement this framework in a real-time scenario.

References

[1]. G. Zhuo et al, "Privacy-preserving Verifiable Set Operation in Big Data for Cloud-assisted Mobile Crowdsourcing", IEEE Internet of Things Journal, 2016.

[2]. V. Jacynyez et al, "Betfunding: A Distributed BountyBased Crowdfunding Platform over Ethereum", 13th International Conference on Advances in Intelligent Systems and Computing, 2016.

[3]. F. Buccafurri et al, "Tweetchain: An Alternative to Blockchain for Crowd-Based Applications",

[4]. M. Ali et al, "Blockstack: A Global Naming and Storage System Secured by Blockchains", USENIX Annual Technical Conference, USENIX, 2016.

[5]. K. Singi et al, "CAG: Compliance Adherence and Governance in Software Delivery using Blockchain", IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain, WETSEB, 2019.

[6]. H. Duan et al, "Aggregating Crowd Wisdom via Blockchain: A Private, Correct, and Robust Realization", IEEE International Conference on Pervasive Computing and Communications (PerCom), 2019.

[7]. J. Xu et al, "Blockchain-enabled Trustless CrowdIntelligence Ecosystem on Mobile Edge Computing", IEEE Transactions on Industrial Informatics, 2019.

[8]. J. Huang et al, "Blockchain-based Crowd-sensing System", Proceedings of 2018 1st IEEE International Conference on Hot Information-Centric Networking, HotICN, 2018.

[9]. P. Yang et al, "Friend is Treasure": Exploring and Exploiting Mobile Social Contacts for Efficient Task Offloading", IEEE Transactions on Vehicular Technology, 2016.

[10]. R. Ouyang et al, "Parallel and Streaming Truth Discovery in Large-Scale Quantitative Crowdsourcing", IEEE Transactions on Parallel and Distributed Systems, 2016.

[11]. A. Azaria et al, "MedRec: Using Blockchain for Medical Data Access and Permission Management", 2nd International Conference on Open and Big Data, 2016.

[12]. D. Peng et al, "Data Quality Guided Incentive Mechanism Design for Crowdsensing", IEEE Transactions on Mobile Computing, 2017.

[13]. K. Yang et al, "Security and Privacy in Mobile Crowdsourcing Networks: Challenges and Opportunities", IEEE Communications Magazine, 2016.

[14]. D. Dang et al, "A Crowdsourcing Worker Quality Evaluation Algorithm on MapReduce for Big Data Applications", IEEE Transactions on Parallel and Distributed Systems, 2016.

[15]. X. Zhang et al, "Keep Your Promise: Mechanism Design against Free-riding and False-reporting in Crowdsourcing", IEEE Internet of Things Journal, 2016.

[16]. 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.