Egyptian Informatics Journal 23 (2022) 405–415

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

Towards developing a Block Chain based Advanced Data Security-Reward Model (DSecCS) in mobile crowd sensing networks

M. Arulprakash *, R. Jebakumar

School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu 603203, India

ARTICLE INFO

Article history:
Received 21 October 2021
Revised 24 February 2022
Accepted 7 March 2022
Available online 12 March 2022

Keywords:
Block Chain
Crowd sensing
Data Security
Reward
Data Privacy

ABSTRACT

Mobile Crowd sensing model is an emerging paradigm that requires mobile device users to perform tasks such as data aggregation and cloud computing operations and also provides significant role in several data-driven applications. For providing effective performance, the crowd sensing model gathers huge data from several mobile nodes in cost-effective manner. Moreover, while handling with high-density sensors, there are several security issues such as, single point of failures, data leakage and so on. Hence, a decentralized ledger mechanism called block chain technology is integrated with crowd sensing models for solving various security concerns, in recent scenarios. With that note, this paper proposes a new model called **Block Chain based Advanced Data Security-Reward Model (DSecCS)** for enhancing data security and attack resistance. Moreover, the mode combines quality of data, status and rewards to make the users to contribute their private data, when dampen the malicious activities. The proposed model comprises of three sections, as, Construction of Intellectual CS Model, Confusion Model and Incorporation of Block-Chain. The experimental results show that the proposed model produces effective results than compared works.

1. Introduction

The Information Technology (IT) and Advanced Communication models are used for observing, sensing, evaluating and integrating distinctive data in Smart Cities for performing intelligent and smooth operations. The applications such as, Smart Transportation, Environmental Protection, Smart Grid, etc, are under Smart City [1]. Moreover, those applications comprises of different and huge varieties of devices such as, sensors, and some other IoT devices for sensing the environment, data transmission and communication through Internet [2]. In recent days, cloud sensing models are widely adopted for providing effective solutions for common data sensing [3]. Moreover, the crowd sensing models are effectively used in effective task execution, pollution control, and so on [4,5].

Mobile Crowd Sensing (MCS) makes the users to communicate on large-scale operations, but also enables with the social features, cloud model and other data. Moreover, communicating with different IoT devices may increase the security risk, and there is no possibility for limiting the privacy settings [6,7]. Several users desire to adopt the IoT products, but, security has become the major threat. Nevertheless, the mobile phases are used to gather the sensing may lead to privacy leakage. Effective User Management and Data Integrity are the significant problems in MCS, which are majorly caused with privacy leakage of users. Most of the entitlements are based on the data quality of users for making others to be participated in the actions. Additionally, rewards are provided to the users based on their data quality, which are processed by the server. Moreover, the works presented in [8–11], the authors have developed incentive mechanisms for MCS, but those works are not concerned about the privacy protection of user data.

For solving the problem, block chain based models are effectively incorporated [12,13], which is a chained structure integrates data blocks in chronological order for ensuring the data security, privacy and integrity. The block chain model has the features such as openness, autonomy, decentralization and so on; hence, many

* Corresponding author.
E-mail addresses: arulpram@srmist.edu.in (M. Arulprakash), jebakumr@srmist.edu.in (R. Jebakumar).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.eij.2022.03.002
1110-8665/

services adopt that for data security. The following Fig. 1 shows the incorporation of block chain in MCS, which comprises of users, Users, Worker and server.

The blockchain technology can be effectively incorporated in mobile crowd sensing, since it can be operated in decentralized manner and also trusted domain [14]. Additionally, the incorporation of BlockChain model makes the model cost effective. And, the anonymity characteristic can protect the user's private data, when they are involved in tasks. For performing that effectively, the Smart Contract [15] can provide the effective task allocation, decentralized reward allocation and user selection, and also process transparent transaction.

1.1. Characteristics of blockchain in MCS

A. Decentralization:

In blockchain, there is no centralized management, in which the distributed storage and accounting.

B. Autonomy:

The model assumes consensus-based protocols for making the nodes to be active for exchanging data in trusted platform.

C. Openness:

The model is considered as open to everyone and anyone can develop applications using the open platform. And, the blockchain model can also be considered as transparent one.

D. No Tampering:

Once the data is checked, validated and stored on to the blockchain, the storage is permanent. Hence, the accountability and data reliability is extremely high in utilizing block chain models.

E. Anonymity:

Since the transaction and communication between nodes are under fixed protocol, there is no requirement for trusted environment.

The main contributions of the proposed model are listed as follows,

1. Proposing a **BlockChain based Advanced Data Security-Reward Model (DSecCS)** for enhancing the user's data privacy, along with protecting the sensing process and reward providence.
2. The security can be effectively achieved by verifying and validating the user identity and the sensing process.
3. Framing the workflow of the proposed model based on smart contracts to aid the process of sensing in MCS. The process is activated once the identities of participants are verified.
4. The reward model ensures that the sensed data is provided by the participants in sustainable manner and the efficacy of the process initiator is enhanced.
5. Analysing the attributes of sensory data market and the users in the work, to improve the reward allocation process.
6. Result analysis based on various security factors to validate the model efficiency.

The remainder of this work is framed as follows: Section 2 deliberates the related work. The complete and clear depiction of proposed work flow is presented in Section 3. The evaluation results are presented with graphs obtained from simulation environment in Section 4. The Section 5 contains the conclusion and future enhancement possibilities in incorporating security over crowd sensing models.

2. Related works

There are myriad works are developed for handling the privacy issues in advanced communication models and transaction services. Crowd sensing is considered as an efficient tool for providing cost effectiveness, utilization of human intelligence and solving distributed issues. Amazon Mechanical Turk (AMT) is a popular crowd sourcing service, which is having several vulnerabilities and possibilities for data leakage [16]. For providing privacy protection in AMT, the authors of [17] developed privacy wrapper. Further, in the work [18], the authors used group signature technique for solving the privacy issues in crowd sensing models. In [19], for effectively handling the data privacy issues, more authorities are used. The distributed authority mechanisms are used to enhance the model trust rate. Moreover, for effectively solving issues related to decentralization, blockchain based models are developed.

In [20], blockchain based security model has been developed, in which privacy protection was not effectively considered and no

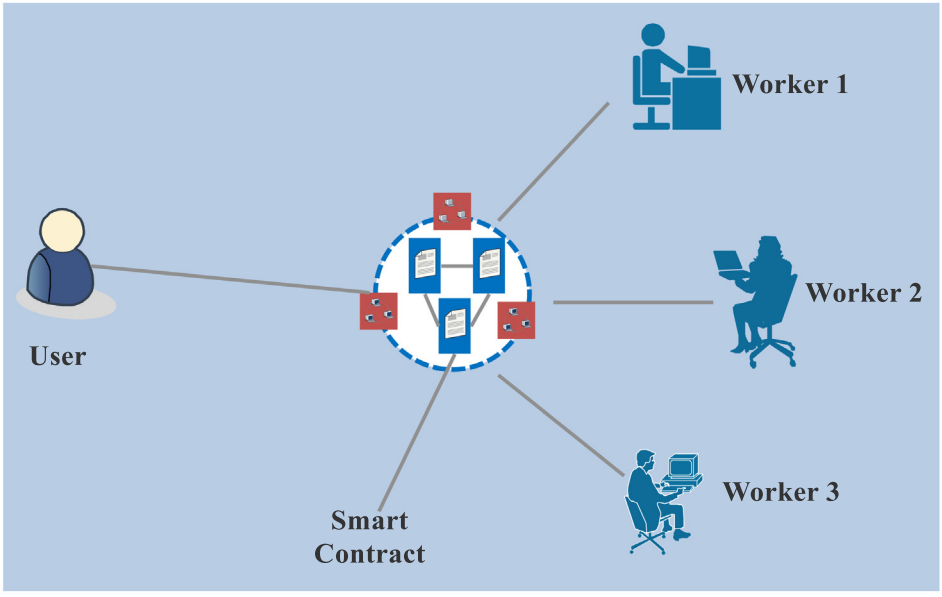

Fig. 1. Block Chain Incorporation in MCS for Data Security.

incentive approached were included. The authors of [21] combined the blockchain as payment gateway for developing a secure communication model, still the privacy protection problems are there in the communication model, specifically, in handling with malicious participants. The model proposed in [22] concentrated on data privacy and anonymity, however, not concerned about the smart contracts and the cost effectiveness. The paper [23] presented an effective survey work based on the incorporation of blockchain models in IoT. Blockchain based participant identity and access management model has been developed in [24], for enhancing the IoT security. Moreover, in [25], IoT model used blockchain method with smart contract declarations were deployed for complex automation process. Object Security Architecture (OSCAR) [26] has been proposed, which provided end to end security based on authentication and authorization models for securing the IoT resource access.

Another survey work has been provided in [27] discussed about the effectiveness of blockchain in IoT based models with the characteristics of decentralization in supporting E-business models. A new model for crowdsensing with blockchain has been developed in [28] for Ethereum. Privacy Preserved Incentive Mechanism has been developed in [29] for crowd sensing networks. The model used encryption algorithm for solving the security problems. In a different manner, the model in [30] developed a Paysense framework that provides rewards for participants and validating the sensed data quality based on the participant's data. The work concentrated on evaluating the user contributing in data sensing, but, complications are noticed in leading to long latency. Further, in [31], the authors developed a trusted cost efficient model that reduces payments in crowd sensing networks. The paper [32] discussed about the limitations in available IoT models and developed a decentralized framework by adopting blockchain based privacy model. Furthermore, the author developed a non-cooperative gaming method for evaluating the competitive environment in nodes.

Fault-tolerant Incentivisation mechanism for peer-to-peer crowd sensing model has been provided in [33]. Further, a token-based smart contract has been developed for efficient task performance and reward providing process using the blockchain based security model. In the work [34], privacy protection has been effectively included with cryptographic functions. The model has taken the monetary incentive model and solving the issues over the cryptographic functions. However, the models discussed in the related woks used traditional incentive mechanisms such as, auction and so on. The models were not effectively utilized the blockchain based security model for data protection. Hence, this inspires to develop a novel method for data privacy protection in MCS networks. The model concentrates on privacy preserving and securing the data sensing process.

3. Working procedure of DSecCS model

The section presents the complete working procedure of the proposed DSecCS Model. And, the Associated blockchain based Crowd sensing model is presented in Fig. 2, which contains two major parts called participants and task managers. The task manager is required for data sensing based on needs. As data provider, the participants are allowed to perform the tasks over bidding. The one who wins are needed to sense the data, upload that and receiving the rewards correspondingly. Moreover, in a typical blockchain model, the messages are given a transactions, in which, the participant 'i' wants to transmit the sensing the data to the crowd. The broadcast operations are performed with the data format, $\{TaskNum, TaskManager, Data, TimeStamp, signature\}$. Moreover, the process appealed with the smart contract, which is processed automatically. And, the task updates of the elements are updated based on Smart Contract. It is significant that the overall transactions are stored in the blockchain.

Here, the task manager is considered as the request, which provides task from various businesses to obtain huge amount of data using crowd sensing. The managers combined and formed to form the associated blockchain. And, as a full node, the manager requires to coordinate the complete blockchain model and functionalities. The participants are the data providers in crowd sensing model. When the participants are authorized, the task sensing process is activated. Furthermore, the participants update the tasks by interacting with the manager.

3.1. System flow

The complete work flow is divided into three sections, Initialization, Task Allocation Process and Model Synchronization. In that, the first part is responsible for required initial settings and authentication, the second section is for processing with crowd sensing operations. And, Model synchronization is for evaluating the issues on data and state processing.

3.1.1. Initialization process

In the proposed model, for ensuring security, digital signature process and smart contract is included in the first phase. Initially, the participant 'i' can forward the registration data to any worker for registration. And, the message data format comprises of $\{Reg, PI_i, PK_i\}$, where, 'PI_i' denotes the participant ID, 'PK_i' is the public key of ith participant. After checking for the authentication of the participant, the manager will produce and transmit the data $RegACK = \{Reg, Hash(PI_i), PK_i, sig_i\}$ to other managers. In this '$Hash(PI_i)$' is the hash function and 'sig_i' is the signature of the manager 'i'. Following, the '*RegACK*' is encapsulated into the blockchain, through which the security is guaranteed. The digital certificate is used as the key for participant 'i' in the crowd sensing model.

3.1.2. Task allocation process

Here, the task allocation process is segmented into four steps, task allocation, selection of participants, data sharing and reward allocation.

A participant 'i' distributes the task observing process by transmitting the task allocation and data sharing, which is given as.

$\{Allocation, TaskNum, Provider, Data, Timestamp, sig_i\}$

The smart contract is invoked for performing the tasks. The TaskAllocation process and transaction is included into blockchain after the agreement between users.

2. After acquiring the data for task allocation, the manager is competing for the participants and provide the rate of bids, which is given as,$\{BidInfo, TaskNo, PartID, Bid_{Price}, TimeStamp, sig_i\}$. Moreover, the manager will consider the user's reliability based on the rate of bid, data and reputation for selecting the participants.

3. After performing that, the participant selection, the winning participant can execute the task and broadcast the sensed data. For enforcing data privacy at this phase, the Public Key Encryption is used for authorized data access. The participant data is encrypted with the symmetric key. When the manager obtains the data, it is decrypted using the private key. For reducing the storage rate of blockchain model, the hashed data is updated.

4. The participants reward is allotted based on the evaluation of data quality. The analysis results are provided and stored in the blockchain and impacts the participant rate_of_reputation.

3.1.3. Model synchronisation

The blockhain is used for synchronization of the functions and participants, since the model is without central administration.

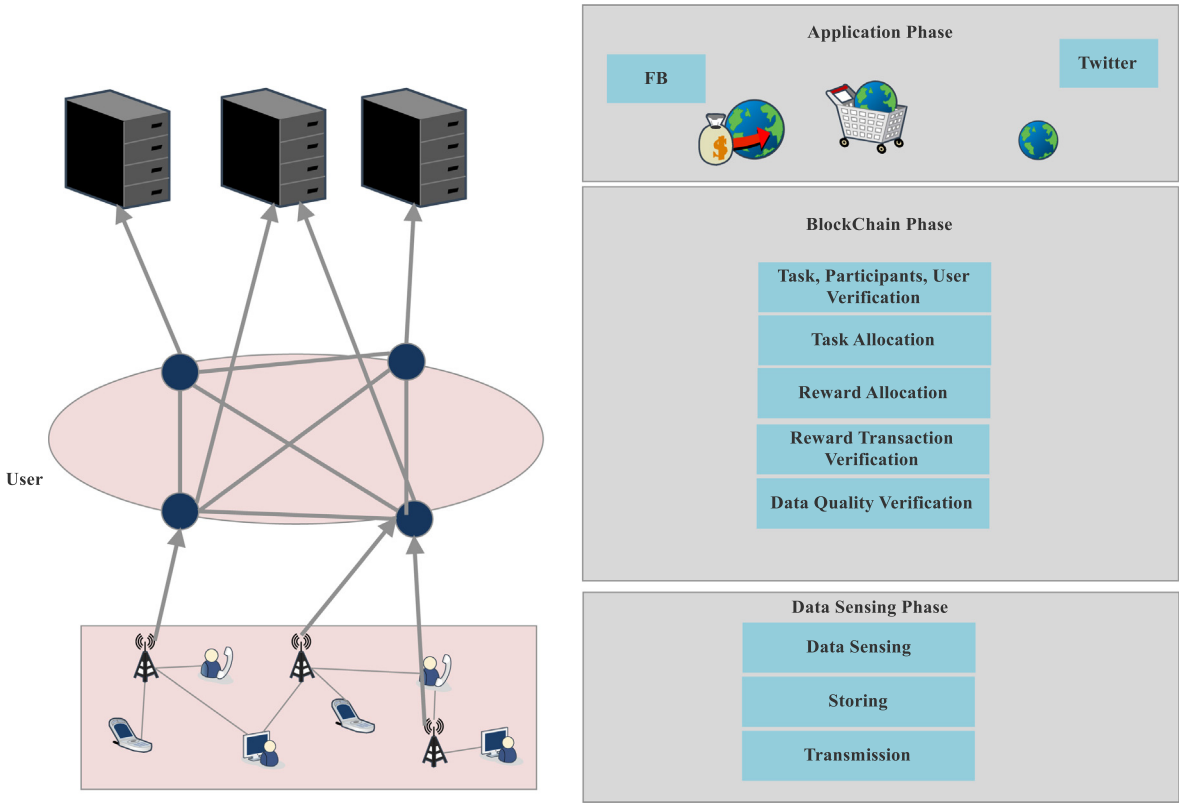

Fig. 2. Associated Blockchain based Crowd Sensing Model with Phases.

The task manager will collect and combine all the valid transaction from user registration and task information to a new data-block, which will be further forwarded to other participants. Following, the new data block is appended to the block chain, ensuring the validity for all data transactions. The Fig. 3 provided the incorporation of blockchain in the communication model. The blocks and the contents are clearly depicted in Fig. 4.

3.2. Smart contracts decriptions

In crowdsensing model, smart contracts are used as an agreement, which provides trust between each user and the model. In this work, it is assumed that the smart contracts are approved before deployment process. Moreover, in this proposed model, a novel Smart Contract (SC-set) is framed for performing the effective communications and verification. And, the SC-set with the model is depicted in Fig. 5.

3.2.1. Registration-based contract

All the users and participants are required to register and the contents are presented in Table 1. The users are requested to register with their address and actions in the secure transaction process for identity verification. Following, the unauthorized users are detected and omitted from the process.

3.2.2. Task observation contract

This contract comprises of the ID, task status, reward modes as presented in Table 2. The task status (TS) is presented in binary state. When the TS is 0, the sensing task in not-finished and, it is 1, denotes the vice versa. There is a factor for providing rewards based on the data quality. And, the factors are given as.

3.2.3. Task execution contract

The maximal gain rate is calculated based on the factors such as task observation, reward allocation and so on. The factors are given in Table 3 for effective task execution.

3.2.4. Reward allocation contract

The reward allocation procedure is the for task sensing, in which the tokens are provided for the participants. And, the factors are provided in Table 4.

3.3. Block chain based advanced data security-reward model (DSecCS)

There are two major issues in selection of participants and reward allocation process. The task manager has no information about the data sensed by the participants before it is shared over the model. Hence, the participants can upload the fake or modified data. In addition, the improper reward providing to participants may reduce the model operations. For solving the above issues, in this work DSecCS is proposed. The first issue is solved considering the factors, present sensed data quality and the participant reputation. And, further, the reward is allocated based on the bid_rate and the inclusive grade for the reasonable reward distribution is processed.

Here, the proposed model is worked on the basis of three significant factors, Bid_rate of participants, reputation, and present data quality. Hence, for solving the multi-factor decision making problem, 'w' is the estimated weight of the bid-rate of all participants, reputation and present data quality. The participant with larger 'w' value has the higher rate of possibility to be selected. And, the computations for total grade of Participant (i) are given as,.

$$\theta_i = w_1 BR_i + w_2 RP_i + w_3 DQ_i \quad (1)$$

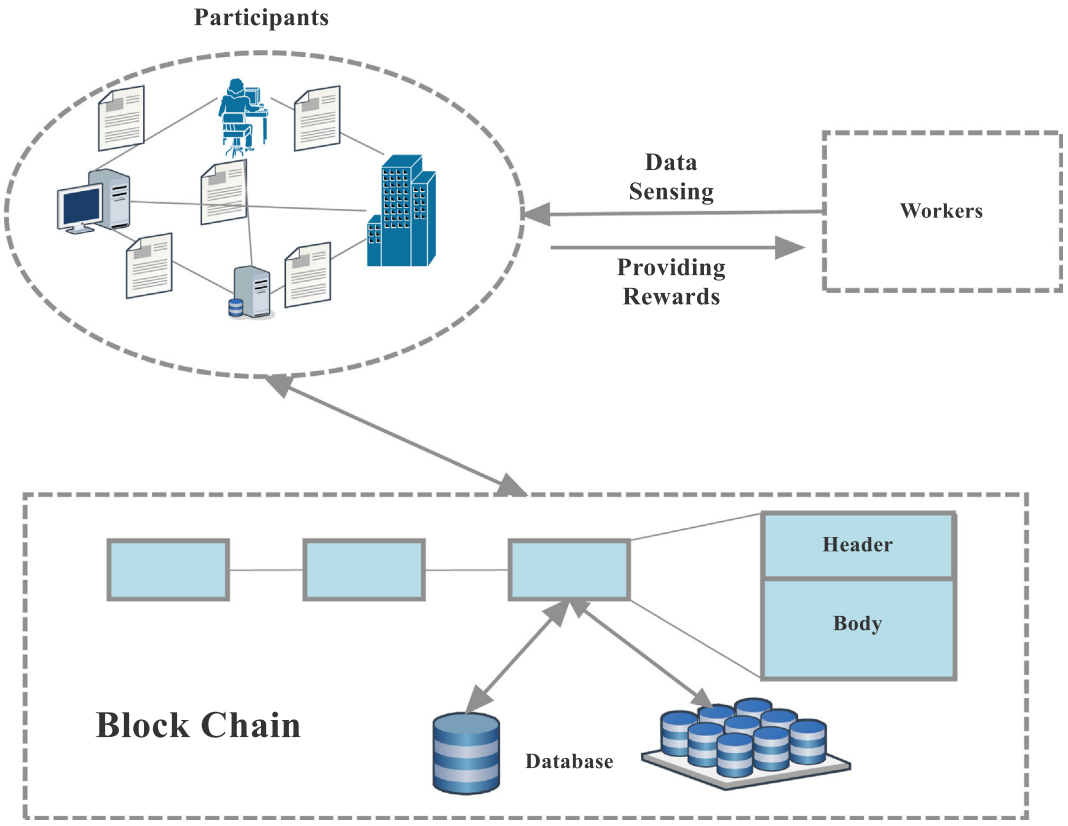

Fig. 3. Incorporation of Blockchain in Crowdsensing Model.

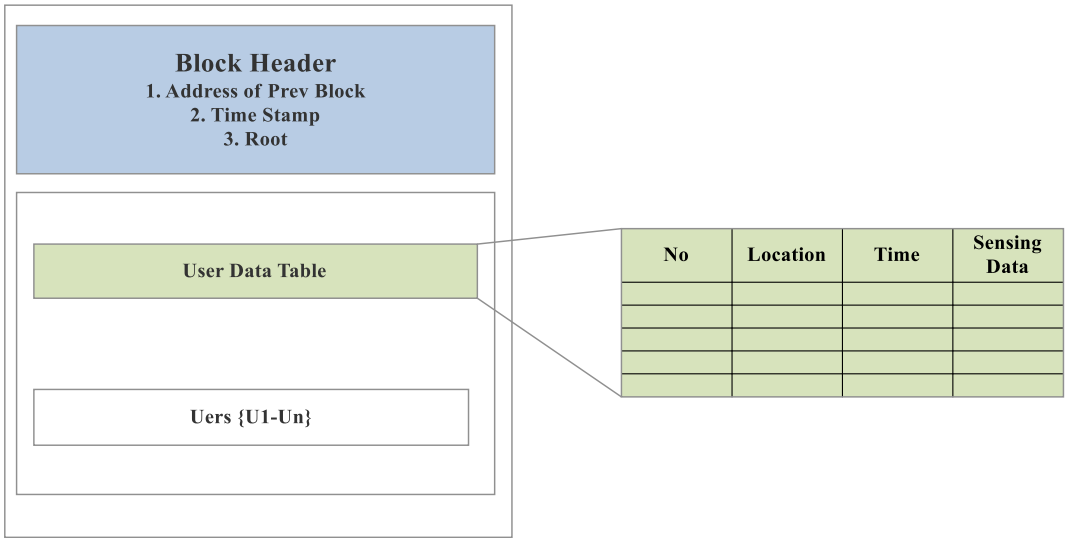

Fig. 4. Structure of Blocks in Blockchain.

where, $w_i \geq 0$, i = 1 to 3, '*BR*' is the bid rate, '*RP*' is the participant reputation, '*DQ*' is the data quality.

3.3.1. Bid_Rate Derivation

On obtaining the task-distribution message, the participants will derive the cost of task processing and provide that for BR. The minimal value of BR, can satisfy the manager, which can acquire the higher rate of probability to be selected, which is given as,.

$$BR_i = 1 - \frac{br_i - \hat{br}}{\acute{br} - \hat{br}} \tag{2}$$

where, $\acute{br}$ and $\hat{br}$ are the maximal and minimal rates of bidding rates. Hence, it is already derived that $\theta_i = w_1(1 - \frac{br_i - \hat{br}}{\acute{br} - \hat{br}}) + w_2 RP_i + w_3 DQ_i$.

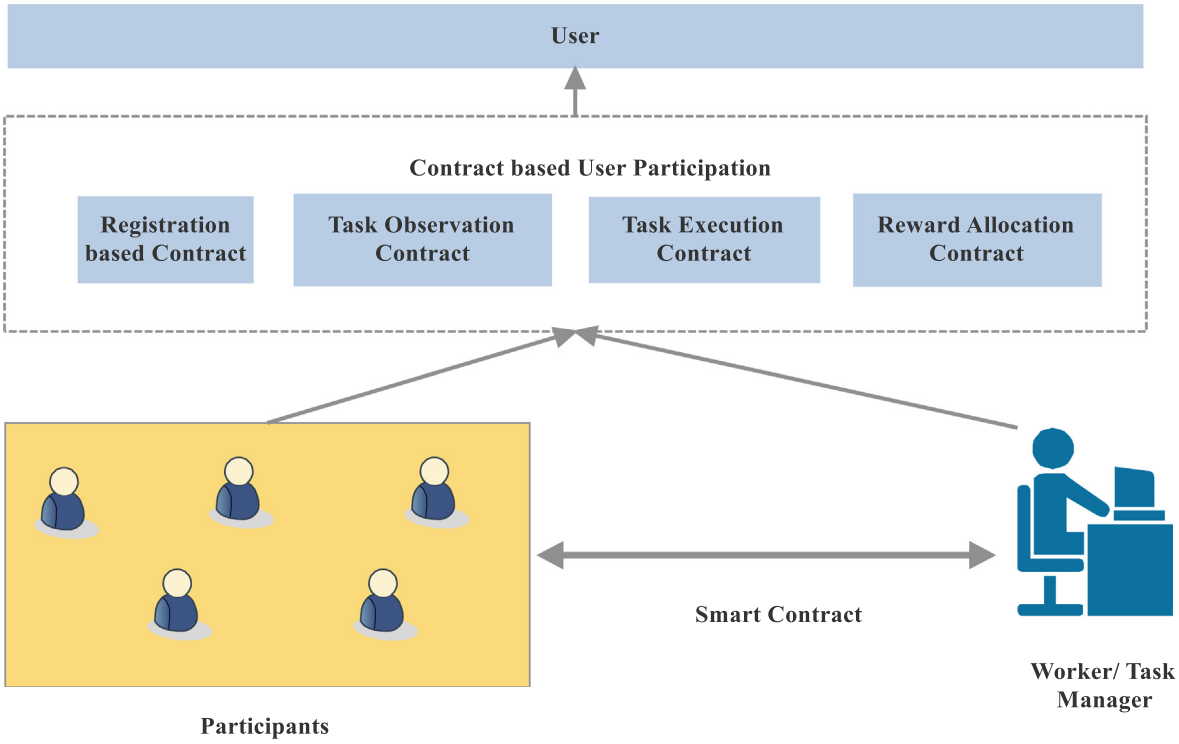

Fig. 5. SC-Set for User Participation.

Table 1
Attributes in **Registration-based Contract.**

Participant ID	Address	Category
PI_1	Addr(PI_1)	Started
PI_2	Addr(PI_2)	Instant User
PI_3	Addr(PI_3)	Monthly User
PI_4	Addr(PI_4)	Yearly User

Table 2
Factor in Task Observation Contract.

Task ID	TS	Reward Mode
T_1	0	RM_1
T_2	1	RM_2

Table 3
Factors in Task Execution Contract.

Participant ID	Gain Rate	Task ID	TS
PI_1	G_1	T_1	0
PI_2	G_2	T_2	1

Table 4
Factors in Reward Allocation Contract.

Task ID	TS	Participant ID	Token
T_1	0	PI_1	TK_1
T_2	1	PI_2	TK_2

3.3.2. Reputation rate Calculation

Any participant can access the 'DQ' for evaluating the participants, to rank the quality rate. Here, the reputation rate can be provided as, good, medium and poor, which can be denoted with, 1, 0 and −1 respectively. And, the computation for each participant is given as,

$$RP_i = \frac{M_i + 1}{M_i + G_i + 2} \tag{3}$$

From (3), 'M_i' denotes the process with good reputation rate and 'G_i' denote the poor rate of satisfactory.

3.3.3. Present data quality

This part denotes the recently transmitted or sensed data quality, which reflects the features of the participants. And, the computation is provided in (4), through which the total grade can be appropriately described.

$$DQ_i = \frac{\sum_{h\epsilon H, k\epsilon k_i}(k) - dq}{\acute{dq} - \grave{dq}} \tag{4}$$

where, 'h' denotes the block height, 'k' denotes the rate of reputation, $\acute{dq}$ *and* $\grave{dq}$ are the minimal and maximal rates of sensed data quality to be considered. It is assumed here, that $P_i(DQ_i)$ is the probability function that the participant 'i' selected by the task manager. When the participant 'i' affirms the bid rate which is nearer to the cost, then,

$$BR_i = \gamma^{-1}(\theta_i) = C_i \tag{5}$$

And, 'θ_i' is submitted to the blockchain, and the remaining participants submit the θ_{-i}. Further, the Conditional Probability for the participant 'i' can be selected and given as,

$$r^* = \delta^{-1}(\theta_i) + \frac{\int_{\theta_{-i}}^{\theta_i} \frac{\acute{br} - \grave{br}}{w_1} P_i(a)da}{P_i(\theta_i)} \tag{9}$$

The computations for participant selection and reward allocation are processed with respect to the derivations given below.

$$p_i(\theta_i, \theta_{-i}) = \begin{cases} 1, if \ \ \theta_i > \theta_{(n-j)} \\ 0, Otherwise \end{cases} \quad (7)$$

where, 'n' is the total number participants in the model. And, the reward allocation is done as,

$$r_i(\theta_i, \theta_{-i}) = \begin{cases} r^*, if \ \ p_i(\theta_i) = 1 \\ 0, Otherwise \end{cases} \quad (8)$$

where,

$$r^* = \delta^{-1}(\theta_i) + \frac{\int_{\theta_{-i}}^{\theta_i} \frac{\dot{br} - br}{w_1} P_i(a) da}{P_i(\theta_i)} \quad (9)$$

Is the reward value of participant 'i', when the participant is selected and, $\theta_{(n-j)}$ represents the highest order of statistic.

4. Results and discussions

The proposed model is implemented in Network Simulation Tool called NS-2 for model evaluation based on factors such as, Storage Overhead, Data Quality, Reputation rate, which impacts greater in model efficiency. Further, the comparative evaluations are carried out based on the parameters such as, Communication overhead, Packet Delivery Ratio (PDR), Packet Drop, and security rates of the model against attacks. Furthermore, the results are compared with the existing models such as, Privacy Preserved Incentive Mechanism (PPIM) and Object Security Architecture (OSCAR) for evidencing the efficacy of the proposed model. And, the initial simulation parameters and domain values are provided in Table 5.

The graph presented in Fig. 6 depicts the result evaluation for Storage Head. As mentioned earlier, the blockchain data contains block header, with 80 bytes and the data for user registration and related information such as, task performance, bidding data and so on. Moreover, the storage overhead of header and task data in one block is given as,.

$$(80 + (150\ 200) \times n) bytes \quad (10)$$

where, 'n' denotes the number of data transactions in each block. Hence, the storage overhead of the complete blockchain is derived as,

$$150.j + (80 + (150\ 200) \times n) * h_0 \ \ \text{bytes} \quad (11)$$

From the results, it can be clearly depicted that the storage cost with the incorporation of blockchain is effective for participants. Following, the Fig. 7 and Fig. 8 shows the results obtained for the evaluations regarding Reputation rate of participants and sensed data quality. The Fig. 9 presents the results of observation about the participants on paid monthly basis and instant users, with respect to the simulation time, corresponding to the size of the sensed data.

Table 5
Simulation Settings and Values.

Parameters	Values
Simulation tool	NS-2.34
Area of coverage	1000 m^2
Time taken for simulation	800 s
No. of Mobile Nodes	Varies from 100 to 1000
End Time of simulation	50 Seconds
Model of Mobility	Random Waypoint
MAC type	IEEE 802.11
Traffic type	CBR
Speed of Mobility	5 m/s
Avg. Hop Distance between Nodes	10 m
Payload Size	512 bytes
Range of transmission between each Node	500 m

4.1. Comparative evaluations

As mentioned before, the comparative analysis are measured based on the factors such as, communication overhead, packet drop, packet delivery ratio, and security rates. The results for communication overhead are presented in Fig. 9. In the proposed model, the model security is effectively handled with blockchain and smart contracts depiction. Hence, the proposed model achieves minimal overhead than the compared models.

The Figures, Fig. 10 and Fig. 11 provide the results derived for Packet Delivery Ratio and Packet drop. For any communication model, the PDR rate should be higher and the rate of packet drop is to be minimal for considering the model is more efficient. It is evidenced from the graphs that the proposed security model in mobile crowd sensing model is more efficient in providing higher rate of PDR and minimal drop rate and provides seamless communication than other compared works (Fig. 12).

Further, the security based evaluations are processed based on two attacks such as collusion attack and tampering attack. Moreover, the evaluations are carried out based on the following considerations.

i. the sensed data can be hacked by the attackers.
ii. the mobile nodes or devices can be malicious.
iii. the communications can be eavesdropped by the attackers.
iv. Data integrity can be affected by the attackers.

With respect to the above consideration, the evaluations are processed, compared with available models and provided the results. The secure rate of the model is computed based on the attack possibilities that can be presented in the process of data sensing.

In Fig. 13, it is considered that the collusion attack is occurred in the process of data sensing and based on that the trust rate of the model is derived. The trust rate of the proposed model is less, when there is the influence of collision attack. With that, the model effectively detects the malicious node behaviour and effectively handles for providing seamless communication over the network.

Based on the aforementioned scenarios, the graph in Fig. 14 depicts the results for tampering attack with the proposed model. By the effective incorporation of blockchain based security, the proposed model detects the malicious behaviours in the communication process. It is clearly given in the Figure that the trust rates are derived accurately by minimal values, and the secure rate shows higher when there is no attacks, which is nearly 1. Therefore, in the scenario of the enforcement of proposed work, the results provide lesser value of secure rate in the presence of attackers, which are to be handled or revoked further for securing the communication in MCS.

5. Conclusions and future work

In this paper, Block Chain based Advanced Data Security-Reward Model (DSecCS) is developed for MCS. Additionally, the model effectively combines the blockchain model for developing the mobile crowd sensing model to can resist various attacks. The utilization of blockchain is for securing the MCS, without considering the third-party authority. Smart Contracts are effectively defined for preventing the fraudulent. Here, the reward allocation is processed based on the factors such as, bidding rate, reputation rate and present data quality. The experimental results show that the model is efficient in all considered network evaluation factors and security factors, than the compared models.

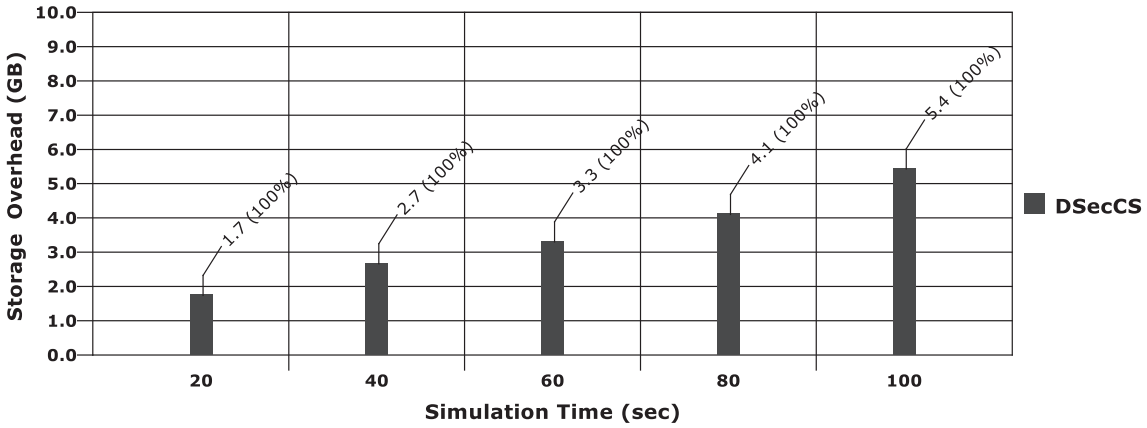

Fig. 6. Storage Overhead Analysis.

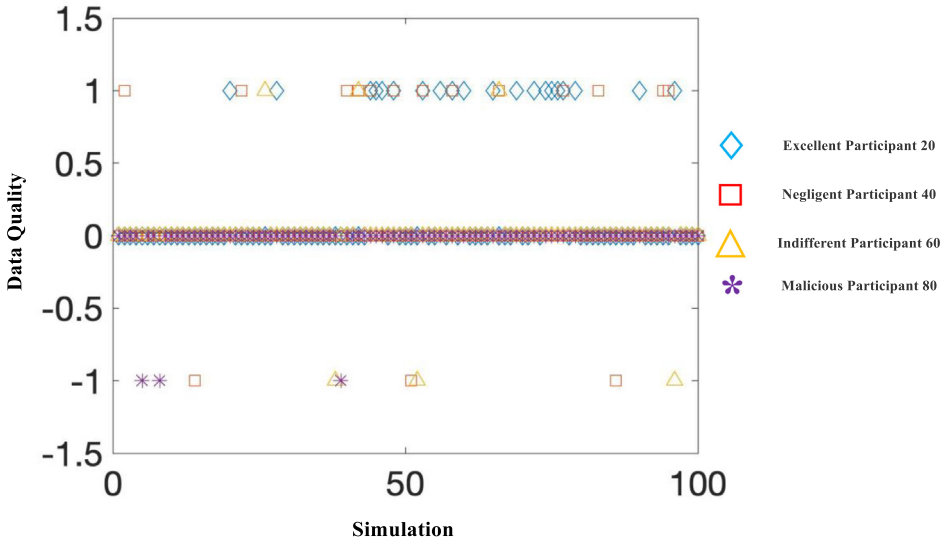

Fig. 7. Sensed Data Quality Vs Simulation.

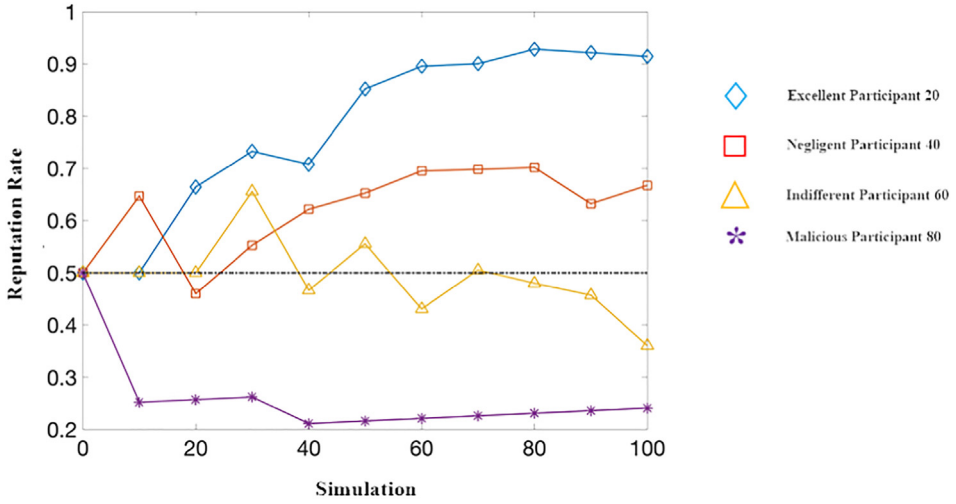

Fig. 8. Reputation Rate Vs Simulation Time in DSecCS.

In Future, the work can be enhanced by considering a static case, where the evaluation metrics of participants are not altered. The model can also be enhanced in such a manner to handle the dynamic changes of user environment. And, methods can also be derived for improving the user privacy with advanced cryptographic models.

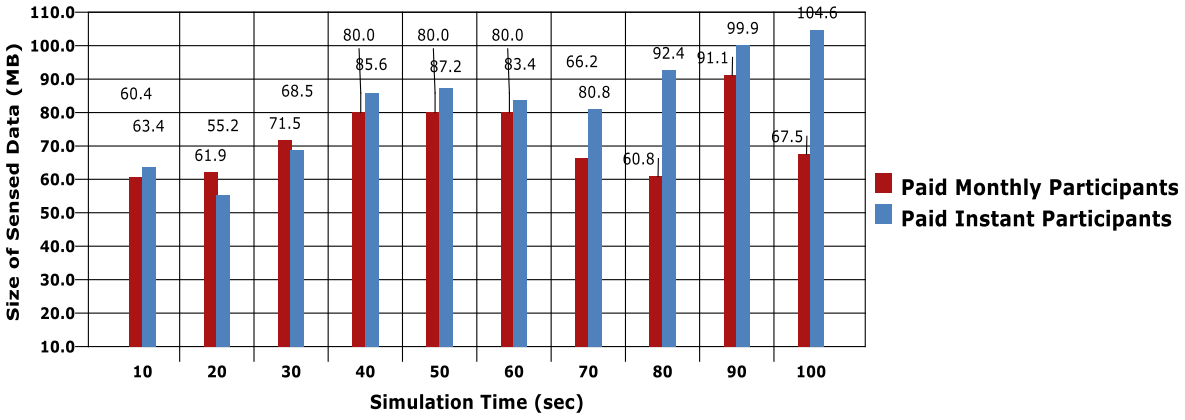

Fig. 9. Participant based Analysis with Blockchain Process.

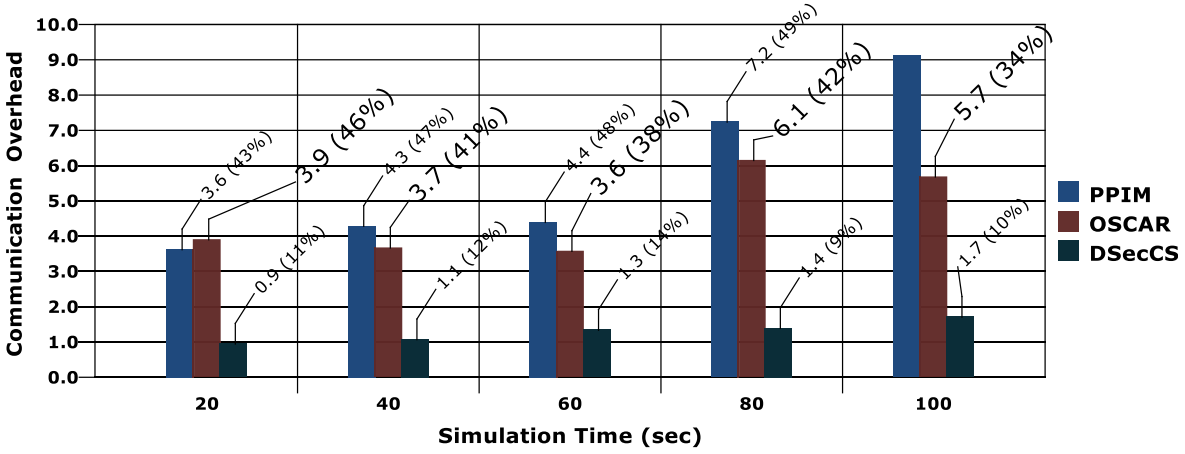

Fig. 10. Communication Overhead based Evaluations.

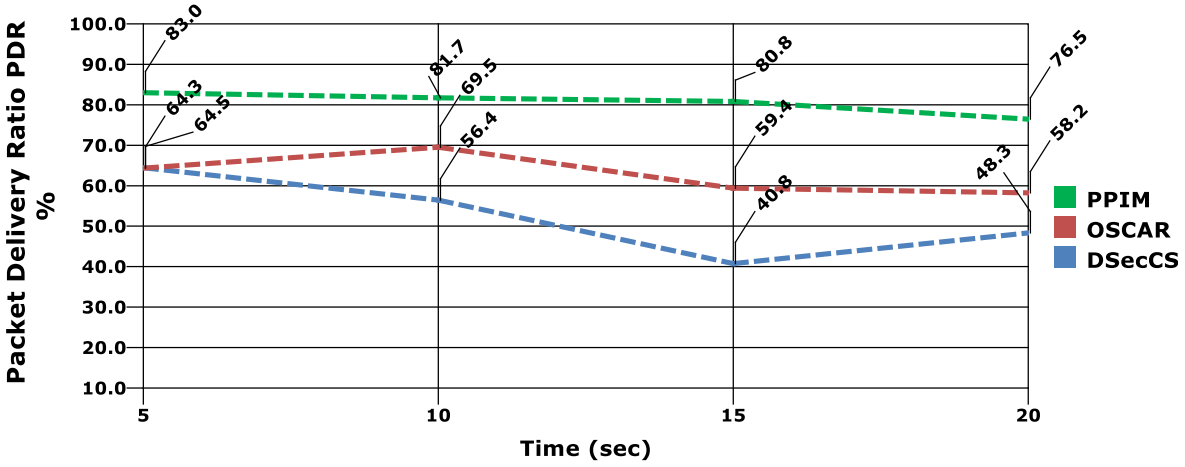

Fig. 11. Packet Delivery Ratio and Results.

6. Conclusions and future work

In this paper, Block Chain based Advanced Data Security-Reward Model (DSecCS) is developed for MCS. Additionally, the model effectively combines the blockchain model for developing the mobile crowd sensing model to can resist various attacks. The utilization of blockchain is for securing the MCS, without considering the third-party authority. Smart Contracts are effectively defined for preventing the fraudulent. Here, the reward allocation is processed based on the factors such as, bidding rate, reputation rate and present data quality. The experimental results show that the model is efficient in all considered network evaluation factors and security factors, than the compared models.

In Future, the work can be enhanced by considering a static case, where the evaluation metrics of participants are not altered. The model can also be enhanced in such a manner to handle the

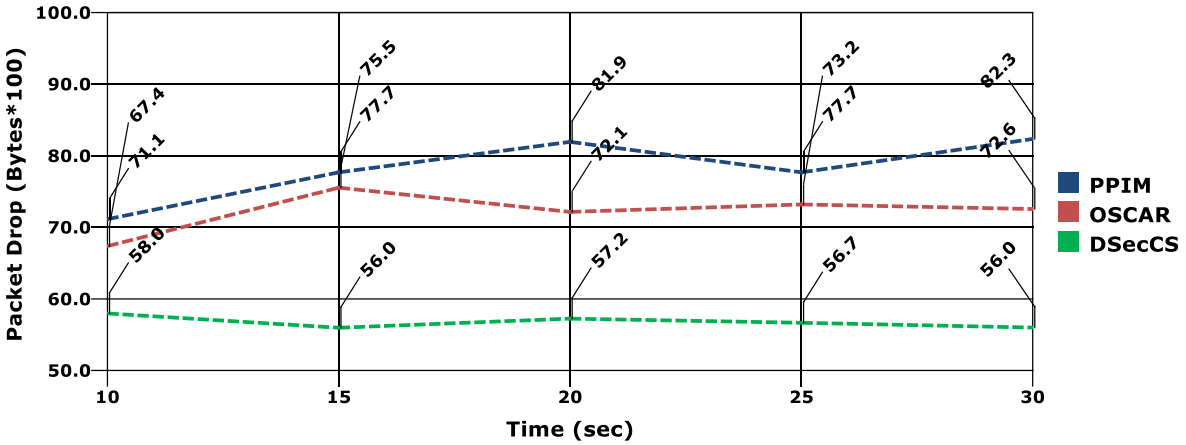

Fig. 12. Packet Drop Analysis among Models.

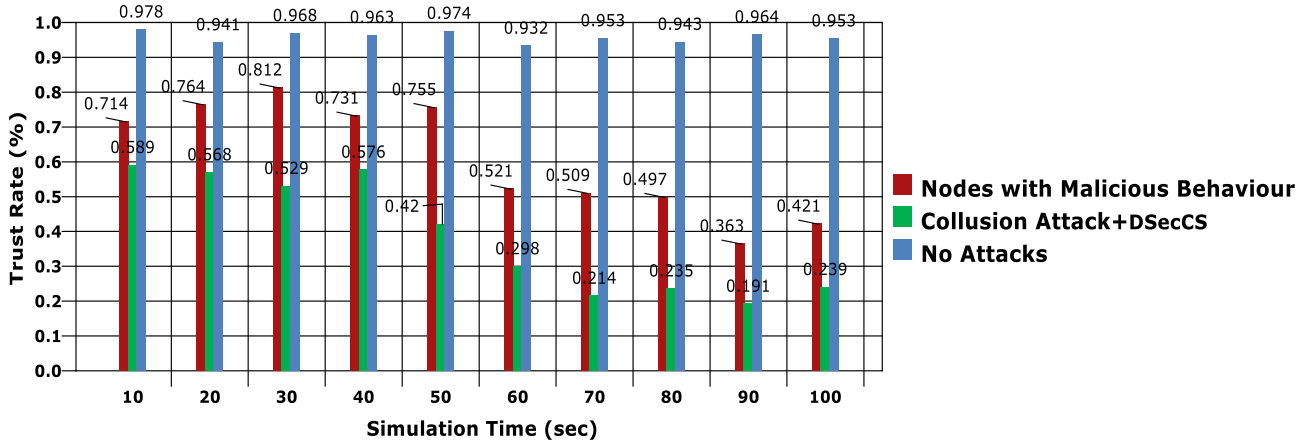

Fig. 13. Security Rate Evaluation with Collusion Attack.

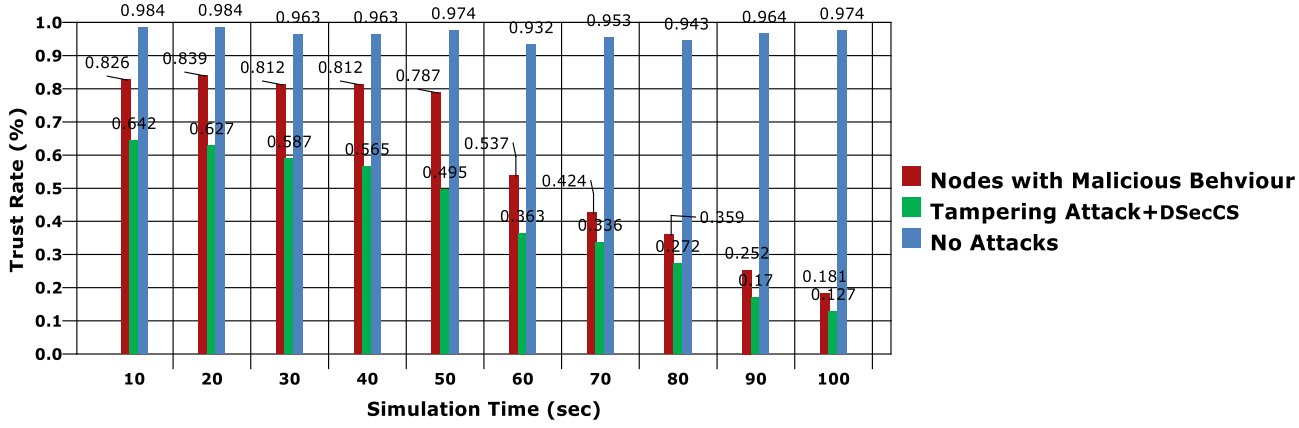

Fig. 14. Security Rate Evaluation with Tampering Attack.

dynamic changes of user environment. And, methods can also be derived for improving the user privacy with advanced cryptographic models.

References

[1] Su K, Jie L, Fu H. Smart city and the applications. In: Proceedings of International Conference on Electronics, Ningbo, 2011, pp. 1028–1031.
[2] Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. IEEE Internet Things J 2014;1(1):22–32.
[3] Longo A, Zappatore M, Bochicchio MA. Collaborative learning from Mobile Crowd Sensing: A case study in electromagnetic monitoring. In Proceedings of the 2015 IEEE Global Engineering Education Conference (EDUCON), Tallinn, Estonia, 18–20 March 2015; pp. 742–750.
[4] Alvear O, Calafate C, Cano J-C, Manzoni P. Crowdsensing in smart cities: overview, platforms, and environment sensing issues. Sensors 2018;18(2):460.
[5] Corradi A, Foschini L, Gioia L, Ianniello R. Leveraging Communities to Boost Participation and Data Collection in Mobile Crowd Sensing. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM),Washington, DC, USA, 4–8 December 2016; pp. 1–6.
[6] Knijnenburg BP, Kobsa A, Jin H. Dimensionality of information disclosure behaviour. Int J Hum Comput Stud 2013;71:1144–62.

[7] Li H, Sarathy R, Xu H. Understanding situational online information disclosure as a privacy calculus. J Comput Inf Syst 2010;51:62–71.
[8] Wen Y, Shi J, Zhang Q, Tian X, Huang Z, Yu H, et al. Quality-driven auction-based incentive mechanism for mobile crowd sensing. IEEE Trans Veh Technol 2015;64:4203–14.
[9] Guo B, Chen H, Yu Z, Nan W, Xie X, Zhang D, et al. TaskMe: toward a dynamic and quality-enhanced incentive mechanism for mobile crowd sensing. Int J Pervasive Ubiquitous Comput Stud 2016:49–52.
[10] Yoshito Tobe, Itaru Usami, Yusuke Kobana, Junji Takahashi, Guillaume Lopez, and Niwat Thepvilojanapong. "vcity map: Crowdsensing towards visible cities". In SENSORS, 2014 IEEE, IEEE, 2014, pp. 17–20.
[11] Zhang Y, Gu, Y, Liu, L, Pan M, Dawy, Z, Han, Z. Incentive mechanism in crowdsourcing with moral hazard. In Proceedings of the 2015 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, 9–12 March 2015; pp. 2085–2090.
[12] Kosba A, Miller, A, Shi, E, Wen, Z, Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP) (2016), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
[13] Swan M. Blockchain: Blueprint for a New Economy; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
[14] Li Z, Kang J, Rong Yu, Ye D, Deng Q, Zhang Y. Consortium blockchain for secure energy trading in industrial internet of things. IEEE Trans Ind Inf 2017.
[15] Nick Szabo. Formalizing and securing relationships on public networks. First Monday, 2 (9) 1997.
[16] McInnis B, Cosley D, Nam C, "Taking a HIT: designing around rejection", mistrust, risk, and workers' experiences in amazon mechanical turk. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, California, 2016, pp. 2271–2282.
[17] Salehi N, Irani LC, Bernstein MS. We are dynamo: overcoming stalling and friction in collective action for crowd workers. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. p. 1621–30.
[18] Rahaman S, Cheng L, Yao DD, Li He, Park J-M. Provably secure anonymous-yet-accountable crowdsensing with scalable sub-linear revocation. Proc Privacy Enhanc Technol 2017;2017(4):384–403.
[19] Gisdakis S, Giannetsos T, Papadimitratos P. Security, privacy, and incentive provision for mobile crowd sensing systems. IEEE Internet Things J 2016;3 (5):839–53.
[20] Li M, Weng J, Yang A, Lu W, Zhang Y, Hou L, et al. CrowdBC: a blockchain-based decentralized framework for crowdsourcing. IEEE Trans Parallel Distrib Syst 2019;30(6):1251–66.
[21] Tanas C, Delgado-Segura S, Herrera-Joancomart J. An integrated reward and reputation mechanism for MCS preserving users' privacy. In: Proceedings of the 10th International Workshop and the 4th International Workshop, Vienna, 2015, pp. 83–99.
[22] Lu Y, Tang Q, Wang G. Zebralancer: private and anonymous crowdsourcing system atop open blockchain. In: Proceedings of the 38th IEEE International Conference on Distributed Computing Systems, Vienna, 2018, pp. 853–865.
[23] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, and Helge Janicke. "Blockchain technologies for the internet of things: Research issues and challenges. arXiv preprint arXiv:1806.09099, 2018.
[24] Kshetri N. Can blockchain strengthen the internet of things? IT Professional 2017;19(4):68–72.
[25] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. IEEE Access 2016;4:2292–303.
[26] Olivier Alphand, Michele Amoretti, Timothy Claeys, Simone Dall'Asta, Andrzej Duda, Gianluigi Ferrari, Franck Rousseau, Bernard Tourancheau, Luca Veltri, and Francesco Zanichelli. "IOTchain: A blockchain security architecture for the internet of things". In Wireless Communications and Networking Conference (WCNC), 2018 IEEE, IEEE, 2018, pp. 1–6.
[27] Zhang Yu, Wen J. The IOT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Network Appl 2017;10 (4):983–94.
[28] Ming Li, Jian Weng, Anjia Yang, Wei Lu, Yue Zhang, Lin Hou, Jia-Nan Liu, Yang Xiang, and Robert H Deng. "2CROWDBC: A blockchain-based decentralized framework for crowdsourcing". IACR Cryptol. ePrint Arch., Univ. California, Santa Barbara, Santa Barbara, CA, USA, Tech. Rep, 444:2017, 2017.
[29] Wang J, Li M, He Y, Li H, Xiao Ke, Wang C. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. IEEE Access 2018;6:17545–56.
[30] Delgado-Segura S, Tanas C, Herrera-Joancomarfı. J. Reputation and reward: two sides of the same bitcoin. Sensors 2016;16(6):776.
[31] Dimitris Chatzopoulos, Sujit Gujar, Boi Faltings, Pan Hui. Privacy preserving and cost optimal mobile crowdsensing using smart contracts on blockchain. arXiv preprint arXiv:1808.04056, 2018.
[32] Shaohan Feng, Wenbo Wang, Dusit Niyato, Dong In Kim, and Ping Wang. Competitive data trading in wireless-powered Internet of Things (IOT) crowdsensing systems with blockchain. arXiv preprint arXiv:1808.10217, 2018.
[33] Shi F, Qin Z, Di Wu, McCann J. MPCStoken: Smart contract enabled fault-tolerant incentivisation for mobile p2p crowd services. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). IEEE; 2018. p. 961–71.
[34] Jia B, Zhou T, Li W, Liu Z, Zhang J. A blockchain-based location privacy protection incentive mechanism in crowd sensing networks. Sensors 2018;18 (11):3894.