Dynamic and Privacy-Preserving Reputation Management for Block chain-Based Mobile Crowd sensing

S. Anto Swaruba[1], A.J. Afin Jenifer[2]

[1]PG Student, Computer Science & Engg, DMI Engineering College, Tamilnadu, India
[2]Assistant Professor, Computer Science & Engg., DMI Engineering College, Tamilnadu, India

---***---

Abstract - *Mobile crowd sensing (MCS) is a rising information assortment worldview that endeavors the potential of individual cell phones to gain mass information in a practical way. One of the significant difficulties in MCS application is to oppose vindictive clients who give bogus information to upset the framework. In the current work, the notoriety the executives conspire is a powerful method to defeat the test. In any case, most notoriety the board plans depends on a semi-legitimate server and procedure information in the plaintext area without thinking about server security and client protection. In this paper, we incorporate the block chain and edge registering in the MCS situation to develop a trustworthy and efficient block chain-based MCS framework, called BC-MCS. To oppose malignant clients, we present a security safeguarding notoriety the executives plot based on the proposed framework. Moreover, we plan an assignment convention to take care of the natural issue of client elements in the MCS. The model framework executed on the Hyper ledger Saw tooth and Android customer exhibits that our plan can accomplish higher utility and security levels in dealing with malignant clients contrasted and the past unified notoriety the executives plans..*

Keywords: **Mobile crowd sensing, reputation management, privacy, block chain, edge computing.**

1. INTRODUCTION

With the fast development of cell phones outfitted with different sensors (e.g., accelerometer, gyrator, camera, and mouthpiece), Mobile crowd sensing (MCS) is proposed to detect and gather information from member clients with the benefits of high volumes information securing and low upkeep cost. In a conventional crowd sensing application, there are three sorts of jobs in the framework: requesters, portable detecting clients (additionally called laborers) and a brought together server. Requesters appropriate detecting errands to the concentrated server, at that point the server initiates a lot of suitable detecting clients to detect and gather information. In the wake of detecting clients transferring detected information, the server totals every single got datum and returns final collection result to requesters In the MCS detecting process, the brought together server planning whole correspondence is excessively amazing without supervision. It isn't known whether the server releases clients' delicate data (e.g., detecting information) or whether it totals detecting information adhering to the standards as specified by the requester. In most existing MCS frameworks, the concentrated server is demonstrated as a semi-legitimate stage, which implies that it executes the endorsed convention sincerely yet is interested about client protection. In reality, be that as it may, the focal server might be noxious as a result of malware contamination or inward assault. When the server is undermined, client protection and collection accuracy can't be ensured. The certificate less cryptographic strategy is a powerful method to beat some security issues of a brought together server, yet it can't fathom the single purpose of disappointment, which is an unavoidable issue for the concentrated server. In this way, the conventional MCS engineering, which depends on a brought together and misty server, is defenseless against noxious assaults and inside bargain.

1.1 MOBILE CROWD SENSING

Crowd sensing, sometimes referred to as mobile crowd sensing, is a technique where a large group of individuals having mobile devices capable of sensing and computing (such as smartphones, tablet computers, wearables) collectively share data and extract information to measure, map, analyze, estimate or infer (predict) any processes of common interest. In short, this means crowdsourcing of sensor data from mobile devices. Devices equipped with various sensors have become ubiquitous. Most smartphones can sense ambient light, noise (through the microphone), location (through the GPS), movement (through the accelerometer), and more. These sensors can collect vast quantities of data that are useful in a variety of ways. For example, GPS and accelerometer data can be used to locate potholes in cities, and microphones can be used with GPS to map noise pollution.

2. PROBLEM DEFINITION

Mobile crowd sensing: Current state was introduced in 2011 by R. K. Ganti [1]. An emerging category of devices at the edge of the Internet are consumer-centric mobile sensing and computing devices, such as smartphones, music players, and in-vehicle sensors. These devices will fuel the evolution of the Internet of Things as they feed sensor data to the Internet at a societal scale. In this article, we examine a category of applications that we term mobile crowd sensing, where individuals with sensing and computing devices collectively share data and extract information to measure and map phenomena of common interest.

Blockchain based efficient and robust fair payment was mentioned in 2018 by R. H. Deng et al. As an attractive business model of cloud computing, outsourcing services usually involve online payment and security issues. The mutual distrust between users and outsourcing service providers may severely impede the wide adoption of cloud computing. Nevertheless, most existing payment solutions only consider a specific type of outsourcing service and rely on a trusted third-party to realize fairness. In this paper, in order to realize secure and fair payment of outsourcing services in general without relying on any third-party, trusted or not, we introduce BCPay, a block chain based fair payment framework for outsourcing services in cloud computing. We first present the system architecture, specifications and adversary model of BCPay, then describe in detail its design. Our security analysis indicates that BCPay achieves Soundness and what we call Robust Fairness, where the fairness is resilient to eavesdropping and malleability attacks. Furthermore, our performance evaluation shows that BCPay is very efficient in terms of the number of transactions and computation cost. As illustrative applications of BCPay, we further construct a block chain-based provable data possession scheme in cloud computing and a block chain-based outsourcing computation protocol in fog computing.

3. PROPOSED WORK

A dynamic and privacy preserving reputation management scheme based on block chain for mobile crowd sensing to overcome the defects of existing schemes. Our contributions are summarized as follows.

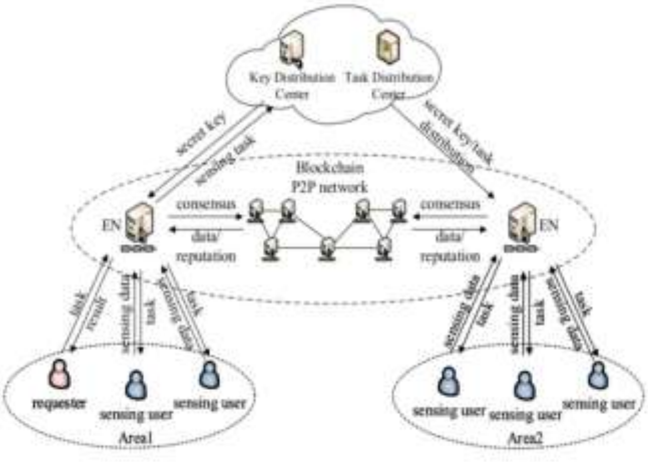

Fig -1: System Architecture

To overcome the security problem of centralized server in traditional MCS application, we utilize block chain technology to propose an efficient BC-MCS system which serves as the open and supervised crowd sensing platform. Based on BC-MCS, we present a practical privacy preserving reputation management scheme in order to defend against malicious users. To preserve user privacy, we design a two-stage reputation update scheme using additive secret sharing without the disclosure of user privacy(sensing data, aggregation result, and requester's feedback) in the public block chain environment. Due to user dynamics in BC-MCS, we improve the basic privacy-preserving reputation management scheme by designing a delegation protocol, so that it has no impact on the system when recruited users leave the system without contributing sensed data. We implement the prototype system of our scheme based on hyper ledger Saw tooth and Android client.

3.1 ISSUE OF KEY AND TASK

First of all, p sends legitimate certificate registered in advance to the KDC and requests the KDC to generate secret key s∈Zp for this sensing task. Then, p publishes the crowd sensing task to the nearest EN.

3.2 SENSING TASK ASSIGNMENT

The sensing task is forwarded to the TDC by ENs.The TDC recruit sn quality sensing users to carry out the crowd sensing task published by p. In addition, p generates n shares from s such that s = s1 +s2 +s3 +□sn, which serve as blinding factors. After that, p distributes n shares to n sensing users via secure communication channel (e.g.,KDC)..

3.3 DATA BLINDING

After receiving crowd sensing task and one share, the recruited sensing users start collecting data with mobile devices. In general, we can suppose that vi is an integer. To achieve the goal of preserving privacy, each sensing user ui utilizes share si to generate blinded data v0 i = vi +si. Then, the blinded data v0 i is encapsulated into a block chain transaction and it is sent to the nearest EN.

3.4 BLOCKCHAIN TRANSACTION VERIFICATION

After receiving block chain transactions from all sensing users, the EN begins to execute smart contract automatically. The EN checks the validity of transactions, including inspecting transaction format, verifying user's signature and auditing the validity of blinded data. The invalid transactions which failed invalidity check are aborted and the valid transactions are recorded in block chain by the EN.

3.5 DATA AGGREGATION

When all sensing users have provided sensing data and ENs have recorded transactions into the block chain, the process of aggregating all sensed data begins to execute as specified in the smart contract. Here the weighted average of all sensing data will be computed by smart contract, where the weight of each sensing data is the sensing user's global reputation score ri stored in block chain publicly. The computed output va is considered as the final aggregation result for requester p. Due to the existence of share in v0 i, we just get the blinded aggregation result v0 a as follows:

$$v'_a = \frac{\sum_{i=1}^{n} r_i \cdot v'_i}{\sum_{i=1}^{n} r_i}$$

3.6 UNBLINDING AGGREGATION RESULTS

We must rely on high precision floating-point calculation to aggregate data. Recall that we assume the sensed data is the integer. This is because the additive secret sharing used in the data aggregation cannot protect the fractional part of decimal data. In the practical scenario, we can use a scaling factor Q which is multiples of 10, to transform fractional data v (sensed data or reputation score) to an integer v = vQ. Afterthe computing completes, the result vresult is scaled down by v result.

4. RESULTS

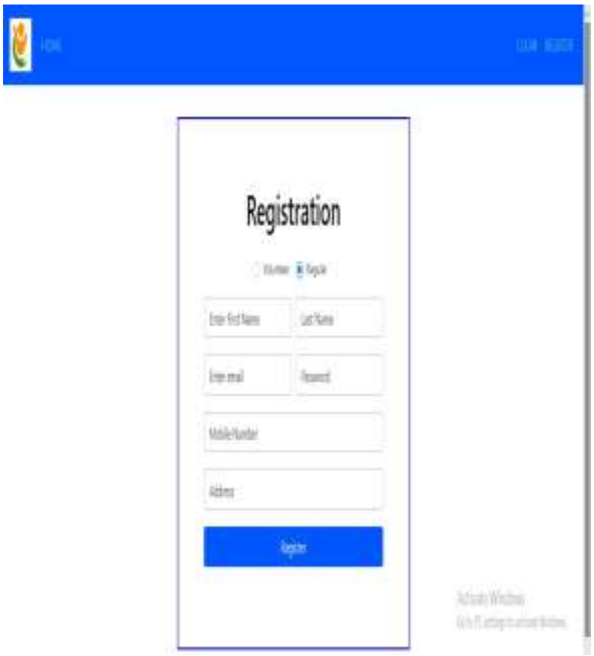

Fig -2: Registration

Fig -3: Login page

Fig 4- User Details

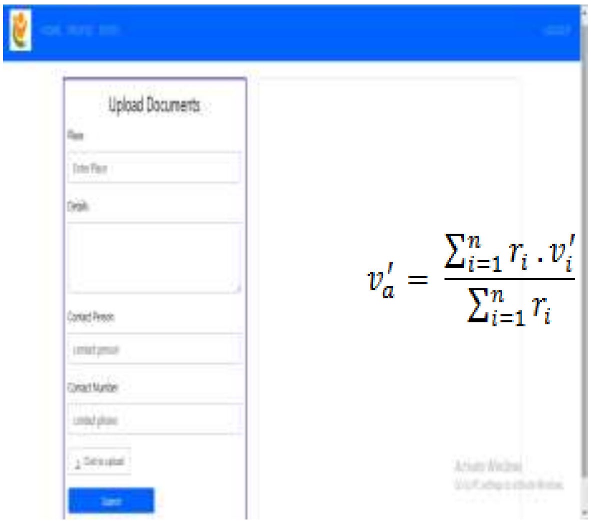

Fig 5- Upload Documents

4. CONCLUSION

The architecture of traditional MCS systems relies on a centralized server which is vulnerable to the threats of internal or external attacks. In this paper, we first integrate block chain and edge computing in MCS scenario and propose a BC-MCS system to carry out sensing task efficiently and resist malicious server. Then, we propose a privacy preserving reputation management scheme to protect user privacy (e.g., sensing data, aggregation result, and requester's feedback) and prevent malicious users simultaneously. Our reputation management scheme consists of local reputation evaluation and global reputation update. In the local evaluation stage, the reliability of user data is evaluated by the degree of data distortion, data consistency, local rating, and contextual factors. The requester gives positive or negative feedback for the user's data service based on data reliability. In the global update stage, the user global reputation scores are updated by smart contract based on the average of all feedback from requesters.

REFERENCES

[1] R. K. Ganti, F. Ye, and H. Lei, ``Mobile crowdsensing: Current state and future challenges,'' IEEE Commun. Mag., vol. 49, no. 11, pp. 3239, Nov. 2011.

[2] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, ``A blockchain based privacy-preserving incentive mechanism in crowdsensing applications,''IEEE Access, vol. 6, p. 1754517556, 2018.

[3] Y. Zheng, H. Duan, X. Yuan, and C. Wang, ``Privacy-aware and efficient mobile crowdsensing with truth discovery,'' IEEE Trans. Dependable Secure Comput., to be published. doi: 10.1109/TDSC.2017.2753245.

[4] Y. Zheng, H. Duan, and C. Wang, ``Learning the truth privatelyand confidently: Encrypted confidence-aware truth discovery in mobilecrowdsensing,'' IEEE Trans. Inf. Forensics Security, vol. 13, no. 10, pp. 2475�2489, Oct. 2018.

[5] A. Karati, S. K. H. Islam, and M. Karuppiah, ``Provably secure and lightweight certi�cateless signature scheme for IIoT environments,'' IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 37013711, Aug. 2018.

[6] Y. Zhang, R. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, ``Efficient and robust certificateless signature for data crowdsensing in cloud assisted industrial IoT,'' IEEE Trans. Ind. Informat., to be published. doi: 10.1109/TII.2019.2894108.

[7] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: Jun. 5, 2018. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[8] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, J.-N. Liu, Y. Xiang, and R. H. Deng, ``CrowdBC:Ablockchain-based decentralized framework for crowdsourcing,'' IEEE Trans. Parallel Distrib. Syst., vol. 30, no. 6, pp. 12511266, Jun. 2019. doi: 10.1109/TPDS.2018.2881735.

[9] F. Shi, Z. Qin, D. Wu, and J. McCann, ``MPCSToken: Smart contract enabled fault-tolerant incentivisation for mobile P2P crowd services,'' in Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jul. 2018, pp. 961971.

[10] C. Cai, Y. Zheng, and C. Wang, ``Leveraging crowdsensed data streams to discover and sell knowledge: A secure and efficient realization,'' in Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jul. 2018,

[11] S. K. A. Hossain, M. A. Rahman, and M. A. Hossain, ``Edge computing framework for enabling situation awareness in IoT based smart city,'' J. Parallel Distrib. Comput., vol. 122, pp. 226237, Dec. 2018.

[12] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, Edgechain: An edge-iot framework and prototype based on blockchain and smart contracts,'' IEEE Internet Things J., to be published. doi: 10.1109/JIOT.2018.2878154..

[13] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, ``Blockchain for secure and ef�cient data sharing in vehicular edge computing and networks,'' IEEE Internet Things J., to be published. doi: 10.1109/JIOT.2018.2875542.

[14] M. Pouryazdan, B. Kantarci, T. Soyata, L. Foschini, and H. Song, ``Quantifying user reputation scores, data trustworthiness, and user incentives in mobile crowd-sensing,'' IEEE Access, vol. 5, pp. 13821397, 2017.

[15] L. Xiao, Y. Li, G. Han, H. Dai, and H. V. Poor, ``A secure mobile crowd sensing game with deep reinforcement learning,'' IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 35�47, Jan. 2018..

AUTHORS

S. Anto Swaruba is currently pursuing her M.E degree in Department of Computer Science & Engineering at DMI Engineering College, Aralvoimozhi, Tamilnadu, India

A. J. Afin Jenifer, currently working as Assistant Professor, Department of Computer Science & Engineering at DMI Engineering College, Aralvoimozhi, Tamilnadu, India.