International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 8, August 2015

Authorized Verification for Distributed Data Storage and Security

[1]Patan Rabbani,[2]S.Vishwanath Reddy
[1]Department of Computer Science and Engineering,Malla Reddy College Engineering and Technology Hyderabad, India.
[2]Asst. professor Dept. of CSE, Malla Reddy College Engineering and Technology,Hyderabad, India
[1]rabbani.patan1234@gmail.com,[2]vishwa.reddy59@gmail.com

Abstract: **Authentication is any process by which a system verifies the identity of a User who wishes to access it. Since Access Control is normally based on the identity of the User who requests access to a resource ,Authentication is essential to effective Security When authentication is required of art or physical objects, this proof could be a friend, family member or colleague attesting to the item's provenance, perhaps by having witnessed the item in its creator's. Data storage security is a wide-ranging area that covers everything from legal compliance, through preparedness for e-discovery requests to user access control and the physical security of data storage. The potential for such data to support scientific discovery and optimization of existing systems is significant, but only if it can be integrated and analyzed in a meaningful way by a wide range of investigators. A novel class of incentive mechanisms is proposed to attract extensive users to truthfully participate in crowd sensing applications with a given budget constraint. The class mechanisms also bring good service quality for the requesters in crowd sensing applications. Although it is so important, there still exists many verification and privacy challenges, including users' bids and subtask information privacy and identification privacy, winners' set privacy of the platform, and the security of the payment outcomes. In this paper, we present a privacy-preserving verifiable incentive mechanism for crowd sensing applications with the budget constraint, not only to explore how to protect the privacies of users and the platform, but also to make the verifiable payment correct between the platform and users for crowd sensing applications. Results indicate that our privacy-preserving verifiable incentive mechanism achieves the same results as the generic one without privacy preservation.**

I. INTRODUCTION

To preserve privacy while mining large amounts of data distributed among different parties, cryptography based privacy preserving distributed data. With the increasing ubiquity of smart phones and their onboard sensing capabilities, crowd sensing as a new paradigm leverages a large number of sensor equipped mobile phones to collect sensing data. The great potential of the crowd sensing offers a variety of novel, efficient ways to enable numerous crowd sensing applications, such as, Nerisel [1],Signal Grugru [2], and V Track [3] for providing omnipresent traffic information, ear-Phone [4] and Noise Tube [5] for making noise maps. To achieve good service quality, incentive mechanisms that motivate smartphone users to participate in these applications are necessary. However, the failure of guaranteeing truthfulness makes traditional incentive mechanisms such as the Viceroy-Clarke- Groves (VCG) mechanism and its variants less attractive [6]–[8]. Nowadays, an emerging class of incentive mechanisms proposed by the authors of [9], [10] has received a widespread welcome and expectancy, since it guarantees the truthfulness, incentive compatibility, budget feasibility and near optimal competitive ratio performance. Although it is promising and truthfulness of users is guaranteed, the truthfulness of the platform has not been fully exploited in the above protocols, which may still make them impractical in real-world crowd sensing scenarios. A common hypothesis made in the above protocols is that the platform will follow the protocols honestly and voluntarily. However, when we observe the platform is operated by rational entities such as an individual within a large corporation, or by a public servant of a government organization. Some entities will not behave correctly and may break the rules of the mechanisms in favor of some users, typically in exchange for bribes, so the hypothesis will be violated. For example, the World Bank recently evaluated the volume of incorrect exchanging hands for public department procurement alone to about US$200 billion per year, with the annual volume of the procurement projects tainted by incorrect operations close to US$1500 million billion. Therefore, how to address the verification challenges brought by the incorrect behavior's of the platform is crucial for the success of crowd sensing applications. In addition to the incorrect behaviors of the platform, privacy issue of both the platform and users is also Challenging in the above incentive mechanisms. If the two privacies of users and the platform are not well protected, both users and the platform will be still reluctant to participate in the crowd sensing

applications. For instance, two privacy concerns emerge in the above mechanisms. The computation of the marginal utility may leak information about current winners' set of the platform to users and also disclose information about subtask selection set of users to the platform since the intermediate winners' set W should be merged with some user ui in one iteration. On the other hand, finding the user with the maximal marginal utility relative to bid by sorting may also disclose various sensitive users bid information and the private information of users' subtask selection preferences. Since huge security and privacy risks are heavily associated with the incentive mechanisms in crowd sensing applications, how to deal with privacy challenges is crucial for the success of crowd sensing applications. Although both verification and privacy issues have been identified as two crucial human factors for realistic crowd sensing applications in MSNs, many recent research works [11]–[14] tend to separately study them in crowd sensing applications. The reason is that, there is an inherent tension between the privacy preservation and the payment verification: both properties are desirable, but they seem contradictory. The winning users procure the payment due to their truthful bids, but they are stymied from verifying the payment because their preferences, behavior abilities, and social profiles are usually kept confidential. At first glance, the dilemma between the payment verification and privacy preservation seems hard to avoid: how can we tell whether the platform is making the payment correctly, without knowing what specifically the platform and other participants did? We believe that existing incentive mechanisms of crowd sensing applications do not have to make this choice, since it is possible, in a sense, to simultaneously attain both the two important goals. Most of existing incentive mechanisms has also only tackled one or the other: they either offer good privacy preservation, with correspondingly weak payment verification guarantees [11], or they preferably trade some privacy for better payment verification guarantees [12]. Therefore, how to simultaneously address the security and privacy issues becomes particularly challenging for realistic crowd sensing application in MSNs. To tackle the above mentioned challenges, in this paper, we first introduce a novel class incentive mechanism for crowd sensing applications in MSNs. Then, we address the privacy preservation of the platform and users by introducing the homomorphism Paillier cryptosystem to compute the marginal utility computation. Furthermore, we prevent bid repudiation by employing a "time-lapse cryptography service". No party, including the platform, receives any information about bids before the mechanism closes, and no user is able to change or repudiate any bid. Finally, we design the privacy-preserving algorithms for the privacy-preserving winner determination and privacy-preserving verifiable payment determination respectively.

II. RELATED WORK

Wireless networks with recent technical advances have become one of the most popular platforms for computing with untrusted for computing with untrusted parties. privacy preservation issues, two crucial human factors in MSNs, have received extensive attentions for crowd sensing applications. Most of reported research works have focused on the selfish issue of users in the incentive mechanisms for crowd sensing applications in MSNs. The authors of [7] focused on the participant's issue of incentive mechanism design for attracting extensive users to provide a good sensing service for crowd sensing applications. Obviously, it is not practical to assume that the requester in their mechanisms will always have an unlimited budget. Recently, the authors of [9], [10], [15] propose a class of promising research works to solve the users' selfishness of practical crowd sensing applications in MSNs. Their incentive mechanisms enhance user participation levels and guarantee users' truthful bids. However, the selfish issue of the platform as well as the privacy issue of the platform and users is neglected. Consequently, users are reluctant to disclosing their bid information and sensing subtasks' selection preferences to others as well as he platform since this may reflect their true valuation and preferences on the sensing subtasks, and the platform are not willing to leak winners' selection set to users as well since this can reduce his revenues. Nowadays, privacy preserving problems have been extensively explored in the context of location based services (LBS) in MSNs. The authors of [16] and [17] introduce the special and temporal cloaking techniques to preserve nodal privacy. Their schemes blur the participant's location at a specific time in a cloaked area or cloaked time interval to satisfy the privacy requirements. Most of these works are based on k-anonymity [18], where a participant's location is cloaked among k - 1 other participant. Furthermore, the authors of [19]–[21] explore the privacy preservation in crowd sensing. The authors of [19] apply the idea of participatory privacy regulation in crowd sensing applications. In [20] and [21], the authors focus on with how participants submit the sensing data to the service provider with revealing their identity. They neglect the following collusion and chatting, which may still result in more privacy leakage. Different from the process of the above anonymous data collection, the authors in [11] preserves the privacy of users by introducing the obvious transfer [22]. However, they do not account for the verifiability of outcomes from the platform. On the other hand, a verification issue from the payment of the platform is also a critical factor faced by the above promising incentive mechanism for crowd sensing applications. An example is the proxy oblivious transfer [23], [24], where users can verify the output of the platform by applying a constructed circuit. The authors of [25] employ a time-lapse cryptography service to keep bidders' bids secure from the auctioneer before the auction closed, and prevent them from

changing their bid after bidding. But their protocol is rather expensive under the condition that there is no collusion between the platform and any user. Recently, a timed commitment is adopted to enhance the levels of the payment security from the platform. For instance, the authors of [13], [14], [26] apply the timed commitment to address the verifiable security issues from different aspects. However, these mechanisms are not applicable in real crowd sensing applications in MSNs, especially the above promising incentive mechanisms. To tackle the above mentioned challenges, in this paper, we address the privacy preservation of the platform and users by introducing the homomorphism, Palliser cryptosystem to compute the marginal utility computation. Furthermore, we prevent bid repudiation by employing a "time-lapse cryptography service" and incentive the platform to comply with the incentive mechanism by checking the payment behavior of the platform.

III. NETWORK AND TRUST MODELS

Network Model-We assume a single owner multi-user large-scale sensor network with N sensor nodes which continuously produce data of interest to many users from both public and private sectors besides the network owner itself. Such sensor networks are under construction or planning by many multi sponsor programs and projects [8]–[10]. There may or may not be an in-network base station bridging the sensor network to the outside network. Our DP2AC can apply to either case for its independence of base station. As in related work [2]– [7], we assume that sensor nodes know their geographical locations which can be acquired via many existing localization schemes.

Authorized Model

Recent years have witnessed a flurry of research activities in securing sensor networks; see for example [13]–[16]. This paper focuses on privacy-preserving access control exerted on users interested in sensed data. We resort to the existing rich literature for other important issues such as key management, secure routing, broadcast authentication, and DoS mitigation. We assume that the network owner charges users for accessing sensed data, thus enforcing strict access control. The network owner is trusted to provide the appropriate amount of data commensurate with users' payments. This coincides with the typical assumption about service providers. It, however, may for various purposes be interested in users' data access patterns, e.g., who are interested in what kinds of data at what locations and time. Although legislative approaches (say, option or opt-out) can be adopted to regulate the collection of such information, it is much more assuring to prevent such privacy-intrusive behavior using sound technical means. Network users are assumed to be selfish, privacy- sensitive, curious, and rational. By selfish, we mean that users always try to pay less for more data given any possible opportunity. For example, they may collude, use forged payments, or even compromise some entities responsible for access control. By privacy-sensitive and curious, we mean that users are reluctant to disclose their own data access patterns but are interested in learning others'. Users are also rational, meaning that they would misbehave only when benefiting from doing so. For instance, we assume that users do not launch DoS attacks on the sensor network because this is against their interest in acquiring useful sensed data. As another example, users do not attempt to evade access control by directly compromising many sensor nodes to read their data, which may require tremendous effort. Instead, users may only compromise a few sensor nodes if doing so could help them reuse tokens.

IV. DISTRIBUTED DATA PRIVACY-PRESERVING ACCESS (THIRD PARTY VERIFICATION) TRD

We outline the DP2AC scheme and defer the details of token-reuse detection (TRD)to DP2AC involves three phases: the initialization phase where the network owner picks security parameters, the withdrawal phase where users purchase tokens, and the spending phase where users spend tokens for data access. Although unable to precisely associate individual tokens with the identities of their holders, the network owner may still narrow down the holder of a particular token to the users who purchased tokens. This might be a concern if the number of token buyers is limited. To overcome this, users may depend on a trusted third party to purchase tokens, thus avoiding submitting payment information directly to the network owner. Alternatively, the network owner can produce token cards; each containing a token covered by a scratch-off panel, and sells them via third parties such as chain stores. Users interested in the sensed data can then purchase token cards using cash or other payment methods if the card seller can be trusted.

Token Spending

The token- spending process is pretty simple. Consider Alice again as an example. After purchasing tokens, Alice (or her agent) can enter the sensor network to acquire data from any sensor node, say node A. Upon receiving a token $\_m, \sigma m\_$, node A first checks $m \stackrel{?}{=} (\sigma m)^e \bmod n$, a standard RSA signature verification. The check should succeed for a genuine token because $(\sigma m)^e = m^{de} = m \bmod n$. If so, A runs the Token-Reuse Detection process to make sure that $\_m, \sigma m\_$ was not used before. Only when $\_m, \sigma m\_$ passes both tests does A provide an appropriate amount of requested data to Alice that is commensurate with the token value. Since A cannot link $\_m, \sigma m\_$ to Alice, it does not know who requested the data as long as Alice does not disclose her identity. Alice's data access privacy is thus well protected. Also note that signature

verification takes an average of 0.7 seconds on TelosB motes [22], which may be significantly shortened if the assembly language optimizations in [23] are used. So this operation is quite affordable in resource-constrained sensor networks.

Oblivious Transfer for Privacy Preservation and Security

Oblivious transfer is a paradigm of secret exchange between two parties, a user and a platform. The user can achieve one of n secrets from the user, without knowing any information about the rest of n secrets, while the platform has no idea which of the n secrets is accessed. Our work employs an efficient 1-out-of-z oblivious transfer of integers [2]. The detailed description is given in the Algorithm Note that regardless of the above signature scheme or oblivious transfer algorithm, they all requires the message to be an integer, therefore, we need to apply $\psi(x) := \lfloor \psi(x) 10k \rfloor$ for the input x, where k can be appropriately chosen to preserve the rank from {3, 4, ・ ・ ・ } and ψ(x) denotes the output of the signature scheme or oblivious transfer algorithm.

Privacy of Users and the Platform

Private information including bids and their assignments might be leaked in three parts: the marginal-utility-per-bid computation, winner selection and payment determination, and the verification of the payment outcomes. Assuming that discrete logarithm is hard, the advantage A dvi of every user ui and the platform in Algorithm S-PVC is less than any positive ε, thereby Algorithm S-PVC is privacy-preserving for users and the platform. *Proof:* In Algorithm S-PVC, the privacy of every user ui may be leaked only in the winner selection part. We prove that adversaries' advantage is negligible in the part below. The privacy of every user ui in this part is related to Paillier encryption algorithm, which is considered provably secure, as its semantic security can be reduced to solving the hard mathematical problem, i.e., the Quadratic Residuosity Problem. Besides, the authors of [34] prove that given a communication string, any value within the input domain has the same probability that it is the encrypted value in the communication sting. Thus, for a given cipher text C, in the operations or sorting of the above three parts, any adversary could not perform better than a random guess, i.e., if the user ui only is given the output.

V. EVOLUATION

The overhead of the computation is summarized in the Table II. To better evaluate the computation overhead, we implemented the S-PVC mechanism in Ubuntu 12.04 using the GMP library based on C in a computer with Intel(R) Core(TM)i5-3470 CPU 3.20GHz. To exclude the communication overhead from the measurement, we generated all the communication strings (cipher text) and conducted all the computation at a local computer. Every operation or protocol is run 500 times to measure the average run time. In general, the S-PVC mechanism consists of the winner selection, the payment determination, and the verification. The winner selection includes users' blind signature, the sorting of the platform and the computation of marginal-utility-per-bid. The payment determination includes the sorting of the platform and the computation of marginal-utility-per-bid. For each user's verification, since data applied to verify the payment are stored in the bulletin board, the computation overhead of the verification is negligible when compared with the above parts. Thus, we do not account for it. Now, we analyze their runtimes respectively.

1) Sorting, Oblivious Transfer and Blind Signature*:* The S-PVC mechanism's run time for one pair of the Nyberg- Rueppel signature including the AI, the platform and users is 28 millisecond on average. Further, we also evaluated the run time of oblivious transfer as well as the final sorting based on the encrypted values. We observed that the signature computation overhead is negligible when compared with the one of the oblivious transfer and the sorting. Users in the S-PVC have much less run time since they only generate the communication strings.

2) Computation of AI, Platform, Winners and Losers*:* We compared the computation overhead of the AI, the platform, winners and losers in when the budget value is 2000. We observed that the computation overhead increase with the budget constraint and at last they were kept in a stable value.

Effect of Budget Constraint on Computation Overhead*:* To evaluate the effects of different budget constraints on computation overhead for each winner ui, we made the experiments to compute the average computation of each winner for different budget values respectively. We needs0.6 microseconds on average, and the overall computation overhead increased with the number of winners and also at last reached a stable value. The computation overhead of each user is very small, thus, we can conclude that the overhead induced by the S-PVC mechanism is applied to wireless mobile devices for crowd sensing applications.

CONCLUSION

In this paper the privacy issues in the distributed computing environments with un-trusted parties. For incentive problems, work has been focused on one important and popular application field, wireless networks, while for privacy issues; this thesis focuses on designing privacy preserving distributed data. Privacy preservation verifiable auction mechanism for crowd sensing application in MSNs. We not only address the privacy preservation of users and the platform by applying the MPEP and oblivious transfer, but also provide a verification scheme for the payment from the platform by using the signature technology and the bulletin board. We

design and analyze the privacy-preserving algorithms for the privacy-preserving winner determination and privacy-preserving verifiable payment determination respectively. Results indicate that our privacy-preserving verifiable incentive mechanism achieves the same results as the generic one without privacy preservation.

REFERENCES

[1] B. Sheng, Q. Li, and W. Mao, "Data storage placement in sensor networks," in *ACM MobiHoc'06*, Florence, Italy, May 2006, pp. 344–355.

[2] W. Zhang, H. Song, S. Zhu, and G. Cao, "Least privilege and privilege deprivation: towards tolerating mobile sink compromises in wireless sensor networks," in *ACM MobiHoc'05*, Urbana-Champaign, IL, USA,May 2005, pp. 378–389.

[3] H. Wang and Q. Li, "Distributed user access control in sensor networks," in *DCOSS'06*, San Francisco, CA, June 2006, pp. 305–320.

[4] D. Liu, "Efficient and distributed access control in sensor networks," in *DCOSS '07*, Santa Fe, New Mexico, USA, June 2007.

[5] W.E. Cobb, E.D. Lapse, R.O. Baldwin, M.A. Temple, and Y.C. Kim, " Transfer of information on Information Forensics and Security" vol. 2, no. 4, pp. 14-24, Dec 2009

[6] K. Ren, W. Lou, and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," in *IEEE SECON'07*, San Diego, CA, June 2007, pp. 223–232.

[7] M. Shao, S. Zhu, W. Zhang, and G.Cao, "pDCS: Security and privacy support for data-centric sensor networks," in *IEEE INFOCOM'07*, Anchorage, Alaska, USA, May 2007, pp. 1298–1306.

[8] Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor networks," *Ad Hoc Networks, Special Issue on Security in Ad Hoc and Sensor Networks*, vol. 5, no. 1, pp. 3–13, Jan. 2007. .

[9] NOPP, http://www.nopp.org/.

[10] IOOS, http://www.ocean.us/.

[11] B. Carbunar, Y. Yu, L. Shi, M. Pearce, and V. Vasudevan, "Query privacy in wireless sensor networks," in *SECON '07*, San Diego, CA, USA, June 2007, pp. 203–212.

[12] K. Ren, W. Lou, K. Kim, and R. Deng, "A novel privacy preserving authentication and access control scheme for pervasive computing environment," in *IEEE Transactions on Vehicular Technology*, 2006.

[13] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in *ACM CCS'03*, Washington, DC, Oct. 2003, pp. 62–72.

[14] H. Chan, A. Perrig, and D. Song, "Random key pre distribution schemes for sensor networks," in *S&P'03*, Oakland, CA, May 2003, pp. 197–213.

[15] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *ACM CCS'03*, Washington, DC, Oct. 2003, pp. 52–61.

[16]Y. Zhang,W.Liu, W.Lou, and Y. Compromisetolerant Fang,"Location-based security mechanisms for wireless sensor networks," *IEEE J. Select. Areas Commun., Special Issue on Security in Wireless Ad Hoc Networks, vol.24,no.2,pp.247-260 feb 2006*