OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

DATA VERIFICATION ALONG WITH ACHIEVING PRIVACY IN ONLINE REVIEWS

Khan Sana Zarrin Masood Khan
PG Student, Computer Science & Engineering Department, EESGOI, Aurangabad

---

Abstract: Abstract: As a significant business paradigm, many online information platforms have emerged to satisfy society's needs for person-specific data, where a service provider collects raw data from data contributors, and then offers value-added data services to data consumers. However, in the data trading layer, the data consumers face a pressing problem, i.e., how to verify whether the service provider has truthfully collected and processed data. Furthermore, the data contributors are usually unwilling to reveal their sensitive personal data and real identities to the data consumers. The proposed a system which finds the contributors are Truthfulness or not using SVM algorithm. In this system user purchase product than he/she can send review to the system than system first check whether the contributors are authorized person or not

---

I INTRODUCTION

1. Ensuring truthfulness and protecting the privacies of data contributors are both important to the long term healthy development of data markets.
2. Therefore, the content of raw data should not be disclosed to data consumers to guarantee data confidentiality, even if the real identities of the data contributors are hidden.
3. It is difficult to guarantee the truthfulness in terms of data collection and data processing, especially when privacies of the data contributors are needed to be preserved.

MOTIVATION

The motivation of the project is TPDM is the first secure mechanism for data markets achieving both data truthfulness and privacy preservation. To integrate truthfulness and privacy preservation in a practical data market, there are four major challenges. The first and the thorniest design challenge is that verifying the truthfulness of data collection and preserving the privacy seem to be contradictory objectives. Ensuring the truthfulness of data collection allows the data consumers to verify the validities of data contributors identities and the content of raw data, whereas privacy preservation tends to prevent them from learning these confidential contents. Specifically, the property of non-repudiation in classical digital signature schemes implies that the signature is unforgeable, and any third party is able to verify the authenticity of a data submitter using her public key and the corresponding digital certificate, i.e., the truthfulness of data collection in our model. However, the verification in digital signature schemes requires the knowledge of raw data, and can easily leak a data contributors real identity To the best of our knowledge, PDM is the first secure mechanism for data markets achieving both data truthfulness and privacy preservation. TPDM is structured internally in a way of Encryptthen-Sign using partially homomorphic encryption and identity-based signature. It enforces the service provider to truthfully collect and to process real data. Besides, TPDM incorporates a two-layer batch verification scheme with an efficient outcome verification scheme, which can drastically reduce computation overhead.

II LITERATURE SURVEY

1. Zhenzhe Zheng,"Trading Data in the Crowd: Profit-Driven Data Acquisition for Mobile Crowd sensing" 2017. As a significant business paradigm, data trading has attracted increasing attention.However, the study of data acquisition in data markets is still in its infancy. Mobile crowdsensing has been recognized as an efficient and scalable way to acquire large-scale data. Designing a practical data acquisition scheme for crowd-sensed data markets has to consider three major challenges: crowdsensed data trading format determination, profit maximization with polynomial computational complexity, and payment minimization in strategic environments. In this paper, we jointly consider these design challenges, and propose VENUS, which is the

first profit-driVEN data acqUiSition framework for crowd-sensed data markets. Specifically, VENUS consists of two complementary mechanisms: VENUS-PRO for profit maximization and VENUSPAY for payment minimization. Given the expected payment for each of the data acquisition points, VENUS-PRO greedily selects the most cost-efficient data acquisition points to achieve a sub-optimal profit. To determine the minimum payment for each data acquisition point, we further design VENUS-PAY, which is a data procurement auction in Bayesian setting[1].

2. Raphael Bost, "Machine Learning Classification over Encrypted Data" Machine learning classification is used in numerous settings nowadays, such as medical or genomics predictions, spam detection, face recognition, and financial predictions. Due to privacy concerns, in some of these applications, it is important that the data and the classifier remain confidential. In this work, we construct three major classification protocols that satisfy this privacy constraint: hyper plane decision, Nave Bayes, and decision trees. We also enable these protocols to be combined with AdaBoost. At the basis of these constructions is a new library of building blocks for constructing classifiers securely; we demonstrate that this library can be used to construct other classifiers as well, such as a multiplexer and a face detection classifier. We implemented and evaluated our library and classifiers. Our protocols are efficient, taking milliseconds to a few seconds to perform a classification when running on real medical data sets[2].

3. Rui Zhang,"Fine-grained Private Matching for Proximity-based Mobile Social Networking" 2012 Proximity-based mobile social networking (PMSN) refers to the social interaction among physically proximate mobile users directly through the Bluetooth/ WiFi interfaces on their smartphones or other mobile devices. It becomes increasingly popular due to the recently explosive growth of smartphone users. Profile matching means two users comparing their personal profiles and is often the first step towards effective PMSN. It, however, conflicts with users growing privacy concerns about disclosing their personal profiles to complete strangers before deciding to interact with them. This paper tackles this open challenge by designing a suite of novel fine-grained private matching protocols. Our protocols enable two users to perform profile matching without disclosing any information about their profiles beyond the comparison result. In contrast to existing coarsegrained private matching schemes for PMSN, our protocols allow finer differentiation between PMSN users and can support a wide range of matching metrics at different privacy levels. The security and communication/computation overhead of our protocols are thoroughly analyzed and evaluated via detailed simulations[3].

4. Magdalena Balazinska, Data Markets in the Cloud: An Opportunity for the Database Community. Cloud-computing is transforming many aspects of data management. Most recently, the cloud is seeing the emergence of digital markets for data and associated services. We observe that our community has a lot to offer in building successful cloud-based data markets. We outline some of the key challenges that such markets face and discuss the associated research problems that our community can help solve[4].

III SYSTEM DESIGN

In the proposed system first efficient secure scheme for data markets, which simultaneously guarantees data truthfulness and privacy preservation. In this system user purchase product than he/she can send review to the system than system first check whether the contributors are authorized person or not. Under a specific data service, this system provides privacy preservation and verifiability.

IV SYSTEM ARCHITECTURE

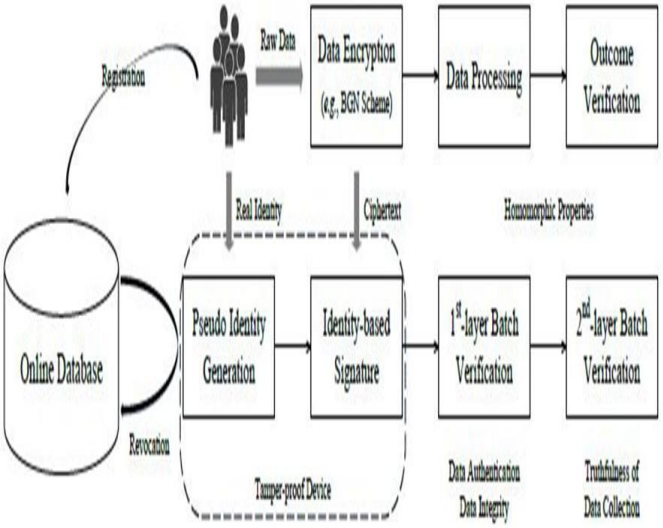

Figure 1: Architecture Diagram

V RESULTS

Figure 2: Home Page

Figure 3: Register-Service Provider

Figure 4: Send Key Request to Registration Center

V CONCLUSION

The data contributors have to truthfully submit their own data, but cannot impersonate others. Besides, the service provider is enforced to truthfully collect and process data. In addition, In this system instantiated two different data services, and extensively evaluated their performances on two real-world datasets. The personally identifiable information and the sensitive raw data of data contributors are well protected.

REFERENCES

[1] M. Barbaro, T. Zeller, and S. Hansell, A face is exposed for AOL searcher no. 4417749, New York Times, Aug. 2006.
[2] 2016 TRUSTe/NCSA Consumer Privacy Infographic US Edition, https://www: truste: com /resources/privacy-research / ncsa-consumerprivacy- index-us/.
[3] K. Ren,W. Lou, K. Kim, and R. Deng, A novel privacy preserving authentication and access control scheme for pervasive computing environments, IEEE Transactions on Vehicular Technology, vol. 55, no. 4, pp. 13731384, 2006.
[4] M. Balazinska, B. Howe, and D. Suciu, Data markets in the cloud: An opportunity for the database community, PVLDB, vol. 4, no. 12, pp.14821485, 2011.
[5] Digital Signature Standard, Federal Information Processing Standards Publication 186, May 1994.
[6] Odlyzko A., Discrete logarithms: The past and the Future; Designs, Codes and Cryptography, (2000), 129-145.
[7] McCurley K., The discrete logarithm problem, Proceedings of Symposia in Applies Mathematica, Vol.42, 1990, 49-74.
[8] Lidl, Niederreiter (1997), Finite Fields (2nd ed.), Cambridge University, Press.
[9] Neal Koblitz, Algebraic Aspects of Cryptography, Springer.
[10] Taher ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE, Transactions on Information Theory, Vol. IT- 31, n.4, 1985, 469-472, also in CRYPTO 84, 10-18, Springer-Verlag.
[11] Lilly P.L, Saju M.I., A method of designing a public-key cryptosystem based on discrete logarithm problem, IRJPA-4(11), 2014, 628-630.
[12] Diffie W., Helman M.E., New Directions in Cryptography, IEEE Transactions on information theory, Vol. IT-22, Nov.1976, 644- 654.
[13] D. Boneh and M. Franklin, Identity-based encryption from the weil pairing, in CRYPTO, 2001.
[14] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469472, 1985.
[15] R. Zhang, Y. Zhang, J. Sun, and G. Yan, Fine-grained private matching for proximity-based mobile social networking, in INFOCOM, 2012.
[16] D. Eastlake and P. Jones, US Secure Hash Algorithm 1 (SHA1), IETF RFC 3174, 2001.
[17] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy, in ICML, 2016.
[18] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in EUROCRYPT, 1999.
[19] X. Meng, S. Kamara, K. Nissim, and G. Kollios, GRECS: graph encryption for approximate shortest distance queries, in CCS, 2015.
[20] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, Generating private recommendations efciently using homomorphic encryption and data packing, IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 10531066, 2012.

[21] C. Niu, Z. Zheng, F.Wu, X. Gao, and G. Chen, Achieving data truthfulness and privacy preservation in data markets, Tech. Rep., 2018. [Online]. Available: https://www.dropbox.com/s/ 7m3jwcio18q4sy0/Technical Report for TPDM.pdf?dl=0

[22] Z. Zheng, Y. Peng, F.Wu, S. Tang, and G. Chen, Trading data in the crowd: Prot-driven data acquisition for mobile crowd sensing,IEEE Journal on Selected Area sin Communications,vol.35,no.2, pp. 486501, 2017.