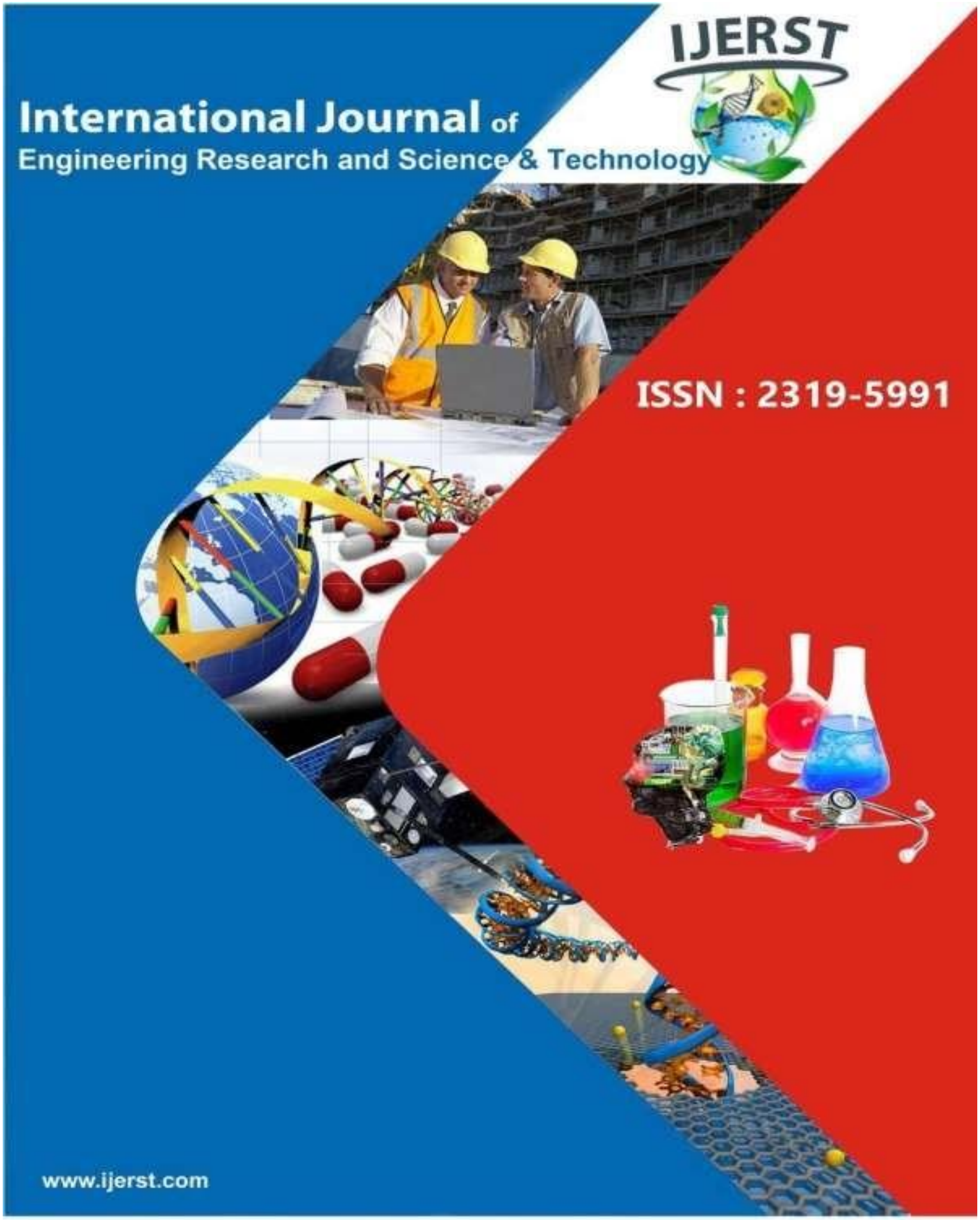


IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

ISSN 2319-5991 www.ijerst.com

Vol. 11, Issue.3, August 2018

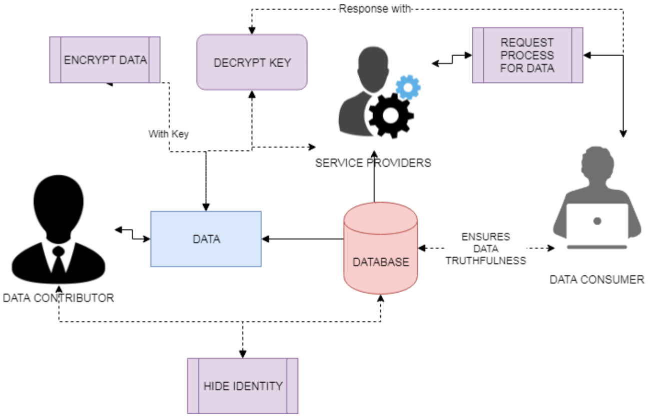
ENSURING DATA TRUTHFULNESS AND PRIVACY PRESERVATION IN DATA MARKET

[1]I.Siva Lakshmi,[2]K. Madhavi,[3]T.Rajesh,[4]D Naga Srinivasulu
[1,2,3]Assistant Professor,[4]Student
Department of CSE
G V R & S College of Engineering & Technology,Guntur,AP

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. In this paper, we propose TPDM, which efficiently integrates Truthfulness and Privacy preservation in Data Markets. TPDM is structured internally in an Encrypt-then-Sign fashion, using partially homomorphic encryption and identity-based signature. It simultaneously facilitates batch verification, data processing, and outcome verification, while maintaining identity preservation and data confidentiality. We also instantiate TPDM with a profile matching service and a data distribution service, and extensively evaluate their performances on Yahoo! Music ratings dataset and 2009 RECS dataset, respectively. Our analysis and evaluation results reveal that TPDM achieves several desirable properties, while incurring low computation and communication overheads when supporting large-scale data markets.

ARCHITECTURE:



EXISTING SYSTEM:

To integrate truthfulness and privacy preservation in a practical data market, there

ISSN 2319-5991 www.ijerst.com

Vol. 11, Issue.3, August 2018

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 contributor's real identity. Regarding a message authentication code (MAC), the data contributors and the data consumers need to agree on a shared secret key, which is unpractical in data markets. Yet, another challenge comes from data processing, which makes verifying the truthfulness of data collection even harder. Nowadays, more and more data markets provide data services rather than directly offering raw data. The following three reasons account for such a trend: 1) For the data contributors, they have several privacy concerns.Nevertheless, the service-based trading mode, which has hidden the sensitive raw data, alleviates their concerns; 2) for the service provider, semantically rich and insightful data services can bring in more profits; 3) for the data consumers, data copyright infringement and datasets resale are serious. However, such a data trading mode differs from most of conventional data sharing scenarios, e.g., data publishing. Besides, the result of data processing may no longer be semantically consistent with the raw data, which makes the data consumer hard to believe the truthfulness of data collection. In addition, the digital signatures on raw data become invalid for the data processing result, which discourages the data consumer from doing verification as mentioned above. Moreover, although data provenance helps to determine the derivation history of a data processing result, it cannot guarantee the truthfulness of data collection.

PROPOSED SYSTEM:

In this Project, by jointly considering above four challenges, we propose TPDM, which achieves both Truthfulness and Privacy preservation in Data Markets. TPDM first exploits partially homomorphic encryption to construct a ciphertext space, which enables the service provider to launch data services and the data consumers to verify the correctness and completeness of data processing results, while maintaining data confidentiality. In contrast to classical digital signature schemes, which are operated over plaintexts, our new identity-based signature scheme is conducted in the ciphertext space. Furthermore, each data contributor's signature is derived from her real identity, and is unforgeable against the service provider or other external attackers. This appealing property can convince data consumers that the service provider has truthfullycollected data. To reduce the latency caused by verifying a bulk of signatures, we propose a two-layer batch verification scheme, which is built on the bilinearity of admissible pairing. At last, TPDM realizes identity preservation and revocability by carefully adopting ElGamal encryption and introducing a semi-honest registration center. We summarize our key contributions as follows. To the best of our knowledge, TPDM 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.

SYSTEM REQUIREMENTS

H/W System Configuration:-

➢ Processor	- Pentium –IV
➢ RAM	- 4 GB (min)
➢ Hard Disk	- 20 GB
➢ Key Board	- Standard Windows Keyboard
➢ Mouse	- Two or Three Button Mouse
➢ Monitor	- SVGA

SOFTWARE REQUIREMENTS:

ISSN 2319-5991 www.ijerst.com

Vol. 11, Issue.3, August 2018

- **Operating system** : Windows 7 Ultimate.
- **Coding Language** : Python.
- **Front-End** : Python.
- **Back-End** : Django-ORM
- **Designing** : Html, css, javascript.
- **Data Base** : MySQL (WAMP Server).

CONCLUSION:

In this paper, we have proposed the first efficient secure scheme TPDM for data markets, which simultaneously guarantees data truthfulness and privacy preservation. In TPDM, 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. Furthermore, both the personally identifiable information and the sensitive raw data of data contributors are well protected. In addition, we have instantiated TPDM with two different data services, and extensively evaluated their performances on two real-world datasets. Evaluation results have demonstrated the scalability of TPDM in the context of large user base, especially from computation and communication overheads. At last, we have shown the feasibility of introducing the semi-honest registration center with detailed theoretical analysis and substantial evaluations.

REFERENCES

1. “Microsoft Azure Marketplace,” https://datamarket.azure.com/home/.
2. “Gnip,” https://gnip.com/.
3. “DataSift,” http://datasift.com/.
4. “Datacoup,” https://datacoup.com/.
5. “Citizenme,” https://www.citizenme.com/.
6. “Gallup Poll,” http://www.gallup.com/.
7. M. Barbaro, T. Zeller, and S. Hansell, “A face is exposed for AOL searcher no. 4417749,” New York Times, Aug. 2006.
8. “2016 TRUSTe/NCSA Consumer Privacy Infographic – US Edition,” https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/.

ISSN 2319-5991 www.ijerst.com

Vol. 11, Issue.3, August 2018

9. 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. 1373–1384, 2006.
10. M. Balazinska, B. Howe, and D. Suciu, “Data markets in the cloud:An opportunity for the database community,” PVLDB, vol. 4, no. 12, pp. 1482–1485, 2011.
11. P. Upadhyaya, M. Balazinska, and D. Suciu, “Automatic enforcement of data use policies with datalawyer,” in SIGMOD, 2015.
12. T. Jung, X.-Y. Li, W. Huang, J. Qian, L. Chen, J. Han, J. Hou, and C. Su, “AccountTrade: accountable protocols for big data trading against dishonest consumers,” in INFOCOM, 2017.
13. G. Ghinita, P. Kalnis, and Y. Tao, “Anonymous publication of sensitive transactional data,” IEEE Transactions on Knowledge and Data Engineering, vol. 23, no. 2, pp. 161–174, 2011.
14. B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, “Privacy-preserving data publishing: A survey of recent developments,” ACM Computing Surveys, vol. 42, no. 4, pp. 1–53, Jun. 2010.
15. R. Ikeda, A. D. Sarma, and J. Widom, “Logical provenance in dataoriented workflows?” in ICDE, 2013.
16. M. Raya and J. Hubaux, “Securing vehicular ad hoc networks,” Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.
17. T. W. Chim, S. Yiu, L. C. K. Hui, and V. O. K. Li, “SPECS: secure and privacy enhancing communications schemes for VANETs,” Ad Hoc Networks, vol. 9, no. 2, pp. 189 – 203, 2011.
18. D. Boneh, E. Goh, and K. Nissim, “Evaluating 2-dnf formulas on ciphertexts,” in TCC, 2005.
19. R. A. Popa, A. J. Blumberg, H. Balakrishnan, and F. H. Li, “Privacy and accountability for location-based aggregate statistics,” in CCS, 2011.
20. J. H. An, Y. Dodis, and T. Rabin, “On the security of joint signature and encryption,” in EUROCRYPT, 2002.