Specialist English: Assignment 9

Rebecca J. Stones
rebecca.stones82@nbjl.nankai.edu.cn

Date due: 20 December 2017

In this ninth assignment (worth 5% of the final mark), we will look at the Conclusions section (or Concluding Remarks) and the references.

My marking will be affected by (a) your English writing, (b) your LaTeX typesetting, (c) your mathematical presentation, and (d) your understanding of the underlying computer science. Basically, I will "peer review" your assignments. (No mark scaling this time.)

Problem 1 In the following three Conclusion sections:

1. describe how the authors go beyond merely summarizing the paper (if at all), and
2. critique how they have done it (i.e., describe the pros and cons, and how they might be improved).

(Item 2. above will vary based on your opinion; I'm seeking reasonably justified answers, rather than a "correct" answer.) [5 marks]

> This article presents the design, implementation, and evaluation of DepSky, a storage service that improves the availability and confidentiality provided by commercial storage clouds. The system achieves these objectives by building a cloud-of-clouds on top of a set of storage clouds, combining Byzantine quorum system protocols, cryptographic secret sharing, erasure codes and the diversity provided by the use of several clouds. Moreover, the notion of consistency proportionality introduced by DepSky allows the system to provide the same level of consistency of the underlying clouds it uses for storage.
>
> We believe DepSky protocols are in an unexplored region of the quorum systems design space and can enable applications sharing critical data (e.g., financial, medical) to benefit from storage clouds. Moreover, the few and weak assumptions required by the protocols allow them to be used to replicate data efficiently not only on cloud storage services, but with any storage service available (e.g., NAS disks, NFS servers, FTP servers, key-value databases).
>
> The article also presents an extensive evaluation of the system. The key conclusion is that it provides confidentiality and improved availability with an added cost as low as 23% of the cost of storing data on a single cloud for a practical scenario, which seems to be a good compromise for critical applications.
>
> — Bessani et al., ACM Trans. Storage, 2013.

> In this paper we presented the design of a toolkit called Cloudmesh that allows to access to multiple clouds through convenient interfaces. This includes command line, a command shell, REST, as well as a graphical user interface. Cloudmesh is under active development and has shown its viability for accessing more than EC2 based clouds. Native interfaces to OpenStack, Azure, as well as any EC2 compatible cloud have been delivered and virtual machine management enabled. An important contribution of Cloudmesh is that it provides a sophisticated interface to bare metal provisioning capabilities that not only can be used by administrators, but also by authorized users. A role based authorization service makes this possible. Furthermore, we have developed a multi-cloud metrics framework that leverages information from various IaaS frameworks. Future enhancements will include network and storage provisioning.
>
> — Laszewski et al., BigSystem, 2014.

> We presented an interactive semantic modeling approach for indoor scenes. The captured indoor scene images are first segmented into regions with object label, and then the segmented objects are replaced by their matched 3D models in the database. As the user continues to capture images of an indoor scene, our system is capable of progressively reconstructing a prototype of the indoor scene. The reconstructed semantic scene can [be] directly applied in computer graphics applications, not only in rendering and gaming which only requires geometry information but also in applications requiring semantic scene information, such as furniture layout.
>
> The limitation of our approach is that the geometry details of the objects are missing in the reconstructed scene. We believe that the similarity between the reconstructed scene and real scene can be significantly improved if the scale of the 3D model database is increased. Recognition accuracy is dependent on the quality of the captured depth data. Although the random regression forest based model matching algorithm can handle noise and partial data well, it still fails to figure out the best matches when the depth data of important features of the objects are missing. Currently, the size of the 3D model database is relatively small, totally 180 models in the database. The scalability of random regression tree based model recognition algorithm to large scale database needs to be further tested in terms of the recognition accuracy and memory footprint.
>
> In the future, we plan to investigate part recognition of the objects in the scene to facilitate deformation of the model in the database to better fit the acquired depth data. We are also interested in various applications of semantic indoor scene modeling, such as context aware augmented reality, virtual indoor decoration and so on.
>
> — Shao et al., ACM Trans. Graph, 2012.

Problem 2 The paper Fu et al. (2017) contains horribly typeset references; it's included on the next page.

1. Rewrite reference [8] (by Lai and others) using BibTeX; the paper is available via: `doi.org/10.1109/TIFS.2013.2271848`. [2 marks]
2. Rewrite reference [13] (by Yu and others) using BibTeX; the paper is available via: `doi.org/10.1109/ICC.2016.7510991`. [2 marks]

Please submit both the BibTeX entry and the compiled reference. The BibTeX entry can be included within a LaTeX file using `\begin{verbatim}` and `\end{verbatim}`, such as in the following example.

```
\begin{verbatim}
@inproceedings{JiQin2003,
  title={Detection of {EEG} basic rhythm feature
    by using band relative intensity ratio {(BRIR)}},
  author={Zhong Ji and Shuren Qin},
  booktitle={Proc. ICASSP},
  pages={429-432},
  year={2003}
}
\end{verbatim}
```

I'm not concerned about what style you use (i.e., `\bibliographystyle{...}`). I personally prefer `\bibliographystyle{siam}`, but this is usually decided by the journal or conference.

Problem 3 In what ways does the typesetting of reference [9] (by Chow and others) differ from the other references? I.e., how is it inconsistent? [1 mark]

Table 1: Comparison of securely outsourcing Matrix Multiplication

	Lei et al.	Our Scheme
Problem Generation	$(m+n+s)\cdot S+$ $(3(m+n+s)+2mn+2ns)$	$k(m+2n+s)\cdot S+$ $(k+1)(mn+ns)\cdot flops$
Problem Verify	$s\cdot S+ns+mn+ms\cdot flops$	$s\cdot S+ns+mn+ms\cdot flops$
Problem Solve	$2(mn+ns)\cdot flops$	$k(mn+2ms+ns)\cdot flops$
Privacy-preserving	×	✓

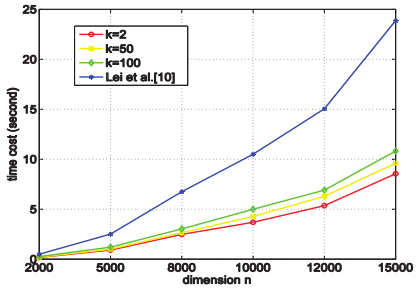

Figure 2: The total running time of our scheme compared with that of [1](m:n:s=4:5:6)

is more efficient than that of our scheme. The experiment results demonstrate that our algorithm is more efficient compared to that of [1].

Remark 3: The choice of k is a tradeoff between security and efficiency. In the proposed algorithm, we suggest that the client can choose k as $k \leq 1\% \min(m,n,s)$.

8. CONCLUSIONS

In this paper, we have presented the security flaw of the algorithm proposed by Lei et al. Although Lei et al. claimed that their scheme is more efficient than others and can achieve security, we have demonstrated that the algorithm cannot protect the number of zero element in original matrices. Therefore, the algorithm cannot preserve the privacy of the outsourced data. We then propose a new privacy-preserving algorithm for outsourcing matrix multiplication computation (MMC) to the cloud. By delegating the most expensive computation of MMC to the cloud, our algorithm relieves the client of its high computation burden. Moreover, with a series of carefully-designed random matrices, our algorithm can properly protect the privacy of input/output data of outsourced MMC. Particularly, it can hide the number privacy of zero elements in the original matrix. Extensive experiments demonstrate that our algorithm achieves higher efficiency than the existing scheme in the client-side computation.

9. ACKNOWLEDGMENTS

This work is supported by the National Nature Science Foundation of China (NSFC) under grant 61379144 and 61572026, Open Foundation of State Key Laboratory of Cryptology (No:MMKFKT201617)and the Foundation of Science and Technology on Information Assurance Laboratory.

10. REFERENCES

[1] Lei X, Liao X, Huang T, et al. Achieving security, robust cheating resistance, and high-efficiency for outsourcing large matrix multiplication computation to a malicious cloud[J]. Information Sciences, 2014, 280:205-217.

[2] Ren K, Wang C, Wang Q. Security Challenges for the Public Cloud[J]. IEEE Internet Computing, 2012, 16(1):69-73.

[3] Lei X, Liao X, Huang T, et al. Cloud Computing Service: the Case of Large Matrix Determinant Computation[J]. IEEE Transactions on Services Computing, 2015, 8(5):688-700.

[4] Chen X, Li J, Ma J, et al. New algorithms for secure outsourcing of modular exponentiations[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(9): 2386-2396.

[5] Wang Y, Wu Q, Wong D, et al. Securely outsourcing exponentiations with single untrusted program for cloud storage[C]//European Symposium on Research in Computer Security. Springer International Publishing, 2014: 326-343.

[6] Chen X, Susilo W, Li J, et al. Efficient algorithms for secure outsourcing of bilinear pairings. Theor. Comput. Sci. 562: 112-121 (2015)

[7] Ren Y, Ding N, Wang T, et al. New algorithms for verifiable outsourcing of bilinear pairings[J]. Science China Information Sciences, 2016, 59(9): 99103.

[8] Lai J, Deng R, Guan C, Weng J. Attribute-based encryprion with verifiable outsourced decryptiončőIEEE Transactions on Informarion Forensics and Security, 2013čň8(8)čž1343-1354čő

[9] Sherman S. M. Chow: A Framework of Multi-Authority Attribute-Based Encryption with Outsourcing and Revocation. SACMAT 2016: 215-226

[10] Wang C, Ren K, Wang J, et al. Harnessing the Cloud for Securely Solving Large-Scale Systems of Linear Equations[C] IEEE International Conference on Distributed Computing Systems. 2011:549-558.

[11] Chen X, Huang X, Li J, et al. New Algorithms for Secure Outsourcing of Large-Scale Systems of Linear Equations. IEEE Trans. Information Forensics and Security, 2015, 10(1): 69-78

[12] Salinas S, Luo C, Chen X, et al. Efficient secure outsourcing of large-scale linear systems of equations[C] Computer Communications (INFOCOM), 2015 IEEE Conference on. IEEE, 2015.

[13] Yu Y, Luo Y, Wang D, et al. Efficient, secure and non-iterative outsourcing of large-scale systems of linear equations[C]//Communications (ICC), 2016 IEEE International Conference on. IEEE, 2016: 1-6.

[14] Lei X, Liao X, Huang T, et al. Outsourcing Large Matrix Inversion Computation to A Public Cloud[J].