Outlook Database under Keyword Common Reliable Internal Rating

B.V. Pranay Kumar
Associate Professor, Christu Jyothi Institute of Technology and Science, Yeshwanthapur

Abstract- **Uploading data streams to a resource-rich cloud server for inner product evaluation, an essential building block in many popular stream applications (e.g., statistical monitoring), is appealing to many companies and individuals. On the other hand, verifying the result of the remote computation plays a crucial role in addressing the issue of trust. Since the outsourced data collection likely comes from multiple data sources, it is desired for the system to be able to pinpoint the originator of errors by allotting each data source a unique secret key, which requires the inner product verification to be performed under any two parties' different keys. However, the present solutions either depend on a single key assumption or powerful yet practically inefficient fully homomorphism cryptosystems. In this paper, we focus on the more challenging multi-key scenario where data streams are uploaded by multiple data sources with distinct keys. We first present a novel homomorphism verifiable tag technique to publicly verify the outsourced inner product computation on the dynamic data streams, and then extend it to support the verification of matrix product computation. We prove the security of our scheme in the random oracle model. Moreover, the experimental result also shows the practicability of our design.**

1. INTRODUCTION

The past few years have witnessed the proliferation of streaming data generated by a variety of applications/systems, such as GPS, Internet traffic, asset tracking, wireless sensors, etc. Retaining a local copy of such exponentially-growing volume of data is becoming prohibitive for resource-constrained companies/ organizations, let alone offering efficient and reliable query services on it.

Consider a stream-oriented service (e.g., market analysis, weather forecasting and traffic management), where multiple resource-constrained sources continuously collect or generate data streams, and outsource them to a powerful external server, e.g. cloud, for desired critical computations and storage savings. For example, using inner product computation over any two outsourced stock data streams from different sources for correlation analysis, a stock market trader is able to spot the arbitrage opportunities. In spite of its merits, outsourcing naturally raises the issue of trust. The third-party server may act maliciously due to insider/outsider attack, software/hardware malfunctions, intentional saving of computational resources, etc. Thus, it is desirable for clients to verify the computation result provided by the server. However, designing a verifiable computation scheme for the above example is not self-explanatory due to the following challenges. First of all, the outsourced computation is data sensitive, i.e., given forged data from a source, the final computation result will be erroneous even if the corresponding query is correctly processed by the server. Cryptography provides an off-the-shelf method to tackle this problem, namely, each data source may be equipped with a unique secret key to "sign" its data contribution, from which traceability is readily derived. However, the typical signature algorithm does not serve on purpose of verifiable multi-key computation. Indeed, most of the existing verifiable computation schemes only focus on the single-key setting, i.e., data and its computation are outsourced from merely one or from multiple contributors but with the same key . On the other hand, we may resort to the powerful fully holomorphic encryption (FHE) but are hardly willing to use it in practice due to efficiency concern . As a result, we are still striving to come up with a promising solution in such a challenging multi-key setting.

2. RELATED WORK

1. Common Clouds to Protect Public Retiring Members:

In this paper, we have a reliable protocol to launch IaaS Domain-based storage in the Virtual Machines and Data Protection process, which is described as an outline. Protocol confidence enables the hardware to be installed by virtual guests' launch of the host platform unveiled and to ensure the confidentiality of a remote storage data, the encryption key excludes the IaaS. Protocol confidence enables the hardware to be installed by virtual guests' launch of the host platform unveiled and to ensure the confidentiality of a remote storage data, the encryption key excludes the IaaS. Experimental results were demonstrated to show the authenticity and efficiency of the proposed protocol. Showing a model that can be included in a tested protocol based cloud environments, model systems implement the implementation of the EHR public bed structure.

2. Survey and analyze data on safety issues with those clouds exercise

IaaS Access to computing resources based on a virtual environment, "cloud", public network, usually provides via the Internet. Resources are meant to calculate virtual server space, network connections, bandwidth, IP addresses and the budget of pregnancy. This will ensure that the integral movable services of profit from IaaS are inspired for this model. Many of the security concerns are because this platform IAs to avoid the benefits of how many companies carry sensitive data. In this paper, the data and explanations of these data functional security plan, IaaS virtual machine as well as preserving the storage launcher currently meet the protocol currently, and the area. The process with theoretical analysis also guides the resistance protocol on the material on the basis of a solid risk model. The tenant enters the virtual machine, and the protocol is encountered remotely configured host platform and it is important that there are encrypted exploits separating the cloud third party storage data. It retained the key out of the IaaS. As a result, the health provokes are shown and can be used in all stages of a third-party process that is efficiently and integrated into cloud environments.

3. Guarantees user security

Resources Operate Rental Hardware Handling - A compact source of flexibility (IaaS) model rental offers the ability to take computing and expand the details and complete free access to complex systems - summary resource, availability of cloud infrastructure. The massive IaaS services on the platforms The possibility of this model is to prove, however, because many companies work with migrant work on platforms to avoid security concerns IaaS for sensitive data functions. In this paper, we have a reliable protocol to describe a frame for IaaS in the data protection process, and to launch virtual machines and protect the field-based storage. We have to continue with theoretical analysis with extensive evidence of the resistance protocol that attacks a specific threat. Protocol confidence enables the hardware to be installed by virtual guests' launch of the host platform unveiled and to ensure the confidentiality of a remote storage data, the encryption key excludes the IaaS. Experimental results were demonstrated to show the authenticity and efficiency of the proposed protocol. Showing a model that can be included in a tested protocol based cloud environments, model systems implement the implementation of the EHR public bed structure.

4. Threats to the security and prevention mechanisms of threats

Why Cloud Computing is a model to come at the service abstract - the demand of the cloud computing network in the IT industry, and that is the debate of the term in the IT industry. Cloud Computing and the various endings in the study provides an overview of potential threats security threats, and risk analysis based on the terms of prevention and company cloud computing cloud of cloud computing, as well as the risk assessment shown on this form. Time goes on, it will be a new security to the problems. This letter showed the author of the analysis based on a detailed survey of the current situation on cloud computing safety issues published.

3 BACKGROUND

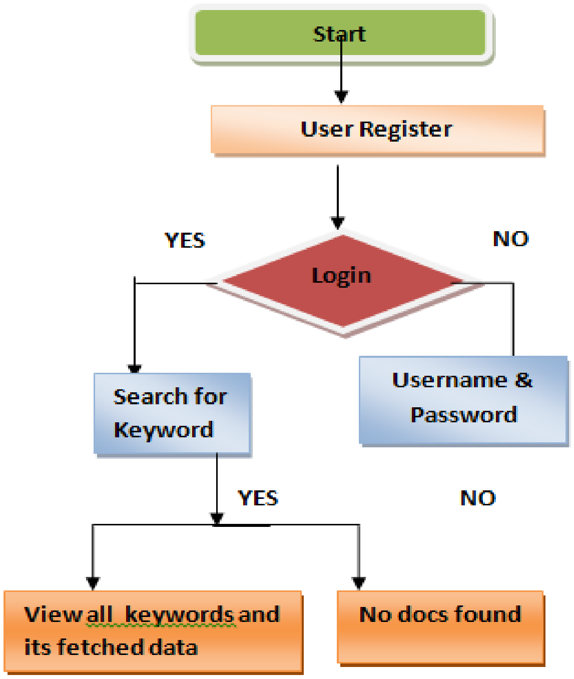
In this paper, we introduce a novel holomorphic verifiable tag technique and design an efficient and publicly verifiable inner product computation scheme on the dynamic outsourced data stream under multiple keys. Our contributions are summarized as follows To the best of our knowledge, this is the first work that addresses the problem of verifiable delegation of inner product computation over (potentially unbounded) outsourced data streams under the *multi-key* Specifically, we first present a publicly verifiable group by sum algorithm, which servers as a building block for verifying the inner product of dynamic vectors under two different keys. Then, we extend the construction of the verifiable inner product computation to support matrix product from any two different sources.

Our scheme is efficient enough for practical use in terms of communication and computation overhead. Specifically, the size of the proof generated by the server to authenticate the computation result is constant, regardless of the input size n of the evaluated function. In addition, the verification overhead on the client side is constant for inner product querie1. For matrix product query, the verification cost is O(n2) in stark contrast to the super-quadratic computational complexity for matrix product.

Our scheme achieves the public verifiability, i.e., a *keyless* client is able to verify the computation results.

We formally define and prove the security of our scheme under the Computational Diffie-Hellman assumption in the random oracle model.

4. SYSTEM FLOW



5. REQUIREMENT ANALYSIS

HARDWARE REQUIREMENTS:

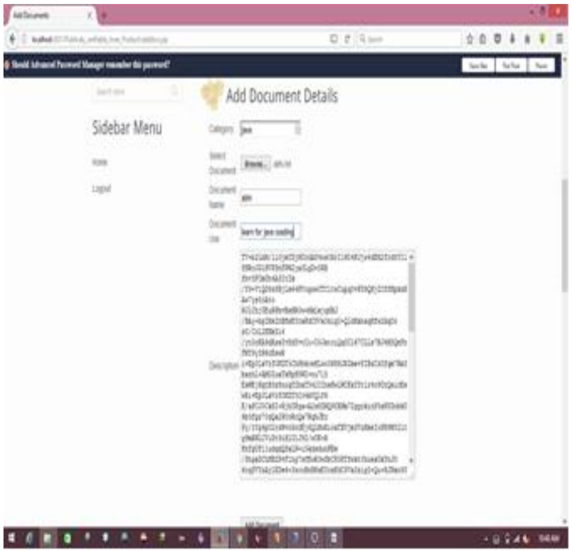
System	:	Pentium IV 2.4 GHz.
Hard Disk	:	40 GB.
Floppy Drive	:	1.44 Mb.
Monitor	:	15 VGA Colour.
Mouse	:	Logitech.
Ram	:	512 Mb.

SOFTWARE REQUIREMENTS:

Operating system:		Windows XP/7.
Coding Language:		JAVA/J2EE
IDE	:	NetBeans 7.4
Database	:	MYSQL

6. EXPERIMENTAL RESULTS

Publicly Verifiable Inner Product Evaluation over Outsourced Data Streams under Multiple Keys
Publicly Verifiable Inner Product Evaluation over Outsourced Data Streams under Multiple Keys
Publicly Verifiable Inner Product Evaluation over Outsourced Data Streams under Multiple Keys
Publicly Verifiable Inner Product Evaluation over



Add Document Details

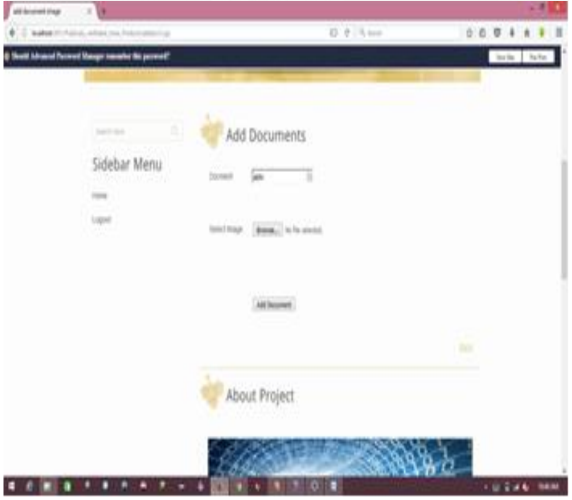
Category: java

Select Document: [illegible]

Document Name: ajm

Document Use: learn for java coding

Description: [illegible]



Add Documents

Document: ajm

Select Image: No file selected.

7. CONCLUSION

In this paper, we introduce a novel holomorphic verifiable tag technique, and design an efficient and publicly verifiable inner product computation scheme on the dynamic outsourced data streams under multiple keys. We also extend the inner product scheme to support matrix product. Compared with the existing works under the single-key setting, our scheme aims at the more challenging multi-key scenario, i.e., it allows multiple data sources with different secret keys to upload their endless data streams and delegate the corresponding computations to a third party server, while the traceability can still be provided on demand. Furthermore, any keyless client is able to publicly verify the validity of the returned computation result. Security analysis shows that our scheme is provable secure under the CDH assumption in the random oracle model. Experimental results demonstrate that our protocol is practically efficient in terms of both communication and computation cost.

8. BIBLOGRAPHY

[1] Y. Zhu and D. Shasha, “Statstream: Statistical monitoring of thousands of data streams in real time,” in Proceedings of the 28th international conference on Very Large Data Bases. VLDB Endowment, 2002, pp. 358–369.

[2] W. Sun, X. Liu, W. Lou, Y. T. Hou, and H. Li, “Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data,” in Computer Communications (INFOCOM), 2015 IEEE Conference on. IEEE, 2015, pp. 2110–2118.

[3] X. Liu, Y. Zhang, B. Wang, and J. Yan, “Mona: secure multiowner data sharing for dynamic groups in the cloud,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182–1191, 2013.

[4] S. Nath and R. Venkatesan, “Publicly verifiable grouped aggregation queries on outsourced data streams,” in International Conference on Data Engineering. IEEE, 2013, pp. 517–528.

[5] D. Catalano and D. Fiore, “Practical homomorphic macs for arithmetic circuits,” in Advances in Cryptology–EUROCRYPT. Springer, 2013, pp. 336–352.

[6] R. Gennaro and D. Wichs, “Fully homomorphic message authenticators,” in Advances in Cryptology-ASIACRYPT. Springer, 2013, pp. 301–320.

[7] M. Backes, D. Fiore, and R. M. Reischuk, “Verifiable delegation of computation on outsourced data,” in ACM conference on Computer and communications security. ACM, 2013, pp. 863– 874.

[8] D. Boneh and D. M. Freeman, “Homomorphic signatures for polynomial functions,” in Advances in Cryptology– EUROCRYPT. Springer, 2011, pp. 149 168.

[9] K.-M. Chung, Y. Kalai, and S. Vadhan, “Improved delegation of computation using fully homomorphic encryption,” in Advances in Cryptology–CRYPTO. Springer, 2010, pp. 483–501.

[10] R. Gennaro, C. Gentry, and B. Parno, “Non-interactive verifiable computing: Outsourcing computation to untrusted workers,” in Advances in Cryptology–CRYPTO. Springer, 2010, pp. 465–482.

[11] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, “Delegating computation: interactive proofs for muggles,” in ACM symposium on Theory of computing. ACM, 2008, pp. 113–122.

[12] J. R. Thaler, “Practical verified computation with streaming interactive proofs,” Ph.D. dissertation, Harvard University, 2013.

[13] S. Benabbas, R. Gennaro, and Y. Vahlis, “Verifiable delegation of computation over large datasets,” in Advances in Cryptology–CRYPTO. Springer, 2011, pp. 111–131.