Open Access Article

PRIVACY-PRESERVING COMPUTATION WITH AN EXTENDED FRAMEWORK AND FLEXIBLE ACCESS CONTROL

V. Rajkumar

Research Scholar, Dept. of Computer Science, AVVM Sri Pushpam College, Poondi, Thanjavur

Dr. V. Maniraj

Research Advisor, PG and Research Dept. of Computer Science, AVVM Sri Pushpam College, Poondi, Thanjavur. (Affiliated to Bharathidasan University) *ORCID ID:* 0000-0002-8113-2616

ABSTRACT

With cloud computing, you have numerous services that are built on data that has been outsourced by employing the tremendous number of resources and tremendous computer power. But it also renders consumers incapable of retaining total control over their personal data. When it comes to keeping data private, users' personal information should be encrypted and sent to the cloud to prevent it from leaking. However, this increases the difficulty of data analysis and access control. Moreover, few existing efforts make use of fine-grained access control for cryptographic computational outputs, which remain out of the reach of many researchers. However, in the process of our prior work, a system for supporting various basic components (such as comparison, multiplication, and addition) was presented that was based on a framework that was more than flexible.

Our framework was designed to support a range of computational tasks while still respecting privacy. To deal with this shortcoming, we present privacy-preserving of four division techniques of computation along with customizable control access. However, here we expand a division technique over integers that is encrypted to provide division on privacy-preserving on other information types, which includes numbers that are either fixed-point (meaning the size is an integer value) or fractional (meaning the size is not a whole number). Finally, we present their proof of security and detail their inefficiency and lack of superiority.

抽象的

借助云计算，您可以拥有大量基于数据的服务，这些数据是通过使用大量资源和强大的计算机能力而外包的。但它也使消费者无法完全控制他们的个人数据。在保护数据隐私方面，用户的个人信息应加密并发送到云端，以防止其泄漏。但是，这增加了数据分析和访问控制的难度。此外，现有的努力很少对加密计算输出使用细粒度的访问控制，这仍然超出了许多研究人员的能力范围。然而，在我们之前的工作过程中，提出了一个支持各种基本组件（例如比较、乘法和加法）的系统，该系统基于一个非常灵活的框架。

Received: August 12, 2021 / Revised: September 08, 2021 / Accepted: September 30, 2021 / Published: October 16, 2021

About the authors：V. Rajkumar

Corresponding author- Email:

我们的框架旨在支持一系列计算任务，同时仍然尊重隐私。为了解决这个缺点，我们提出了四种计算划分技术的隐私保护以及可定制的控制访问。然而，这里我们扩展了对整数的除法技术，该技术被加密以提供对其他信息类型的隐私保护的除法，其中包括定点数（意味着大小是整数值）或小数（意味着大小是不是整数）。最后，我们展示了他们的安全性证明，并详细说明了他们的低效率和缺乏优势。

INTRODUCTION

Using the large volume of resources and powerful computation of the Internet, cloud computing is an excellent way to memory and data process. As it is the advent of the IoT brought about the requirement for large data generation, analysis, and processing, this has created a significant amount of compute overhead that cannot be handled by locally connected devices. In the first place, encryption hinders the processing and analysis of data, especially when it comes to division.

Homomorphic encryption, in the case of operations over encrypted data, allows partial/full homomorphic encryption to be applied, but because of this, homomorphic encryption methods can only the operations that is supported such as multiplication and addition on encrypted data. Second, the flexible restriction of access to outsourced data computing outcomes remains an unresolved question.

The majority of present homomorphic encryption methods support the results only by a single user. There are divisions that are missed, as the computation is difficult. In order to increase the ease of use, scalability and flexibility of our framework, we employ an extension and complementing approach for the building upon our existing system architecture and applying privacy-preserving division computation.

RESEARCH PROBLEM

This division function is a new addition to our earlier work, making our previous data protection system more generic and adaptable.

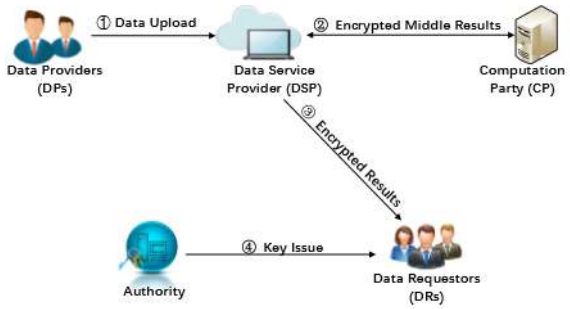
1) The data storage and computational service supplied by a cloud server is performed by a data service provider (DSP).

2) CP can be a data computation and access control department, which generally offers cloud computing and data processing services.

3) Data Providers (DPs) are cloud service users who gather, produce and download data to DSP. so that the DSP can store and process it quickly and efficiently.

4) Data consumers (data requesters) are people who are interested in getting the outcomes of data processing. A DP is also a DR.

5) With authority in control of critical management, authority is totally trusted.



The system follows protocols, but entities nevertheless attempt to explore others' data. Additionally, we believe that the DSP and the CP will not work together as they will both suffer from worse reputation and greater profit loss if they do. The introduction of the adversary A*

here shows that this is not an attack, but rather an attack simulation.

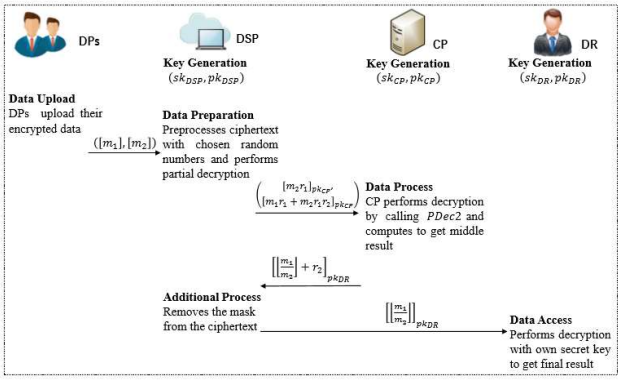
The objective of this project is to get raw data by confronting data consumers with special abilities (either a dumper or a data pump).

1) A^* has the ability to intercept all channels save those between the Authority and its users, so it can gain access to the communications that have been sent on those channels.

2) A^* could be potentially compromise its DSP or CP in order to gain raw data by guessing ciphertexts.

3) A^* Compromising one DSP and certain DPs in order to arrive at the final processing results could potentially result in compromising of the system.

4) A^* an algorithm could compromise a DSP or CP, which in turn compromises the DR, so that the DR is unable to correctly reconstruct the original data. Even the opponent A^* cannot compromised the DSP and the CP at the same time nor can the challenged DR or DP compromise.



LITERATURE SURVEY

Arithmetic Transformations Based on Secure Division

Katzenbeisser et al. [1] pick a tuple (ρ_x, σ_x, τ_x) to present a value χ which based on a certain interval $[-l; +l]$ with $l > 0$, where ρ_x is a nonzero flag, σ_x the sign of the value is encoded x and τ_x represents the accurate of the value. For computing the division result, you can use fundamental operations such as addition and subtraction on corresponding elements and apply a function $LDIV([\bar{x}], [\bar{y}])$.

Though numbers can be used to do computations on integers, their ultimate division calculation is approximate with a relative inaccuracy that is bounded and encoding increases processing overhead. This difficulty must be overcome in order to receive an absolute result, Dahl et al. [2] transformed the Divide calculations into multiplication over encrypted data and add them to encrypted data using a Taylor expansion of the denominator reciprocal. In the era of personal data, privacy-preserving computation seeks to bridge this gap: to exploit data while keeping the personal information of individuals private.

A division mechanism to handle encrypted floating-point numbers was developed by Ugwuoke et al. [3] to help compensate for this issue. In all of the above two division systems, iterative computations that yield a fixed precise result use fixed rounds of calculations to provide a fixed result, which results in a high computational cost.

Privacy preserving computation effectiveness

For sensitive and personal cloud-IoT applications, there are two core expectations: usefulness and privacy. Complicated cloud-IoT ecosystems have seen an increasing worry about data utility at the expense of privacy. However, current best practices for securing privacy include methods that prevent users from doing meaningful work with encrypted data. That's still up in the air, because we're trying to find a solution to this puzzle: "How can cloud computing help IoT device users stay safe and private?" Fully homomorphic encryption (FHE)

encryption techniques can be used by cloud service providers (CSPs) to construct privacy-preserving services.

In fact, cloud-IoT devices have their own unique issues. To assist deploy FHE based solutions in the real world, we have thus established a service structure that we term proxy reciphering. For secure IoT-device data calculations, we use strategies like supplied servers, chameleon hash, FHE, and secret sharing functions to produce an algorithm that's secured Even after a compromise key device. We create a testbed and run real-world ECG records from TELE ECG database to measure the latencies in the framework.

Secure Division Based on Bit Decomposition Protocol

The modulo value action restricts the length of the data in the division computation. You can use random numbers for both the dividend and the dividend to ensure their secrecy. To acquire an absolute quotient, the data masked is difficult to calculate. A combined result can be obtained while keeping the data inputs secret by utilizing secure multi-party computing (SMPC). Computation such as advanced machine learning algorithms is now supported by SMPC techniques, which have seen a substantial improvement in efficiency in recent decades. Therefore, several research employ the technique for secure bit decomposition (SBD.

First, the cloud decrypts encrypted data as binary string before performing bit shift operations to generate a quotient and a remainder. However, it is often difficult to deploy the bit decomposition protocol. Finally, of all the books on this list, all of them ignore the restrictions on division results from ciphertext. In our previous effort, we achieved this aim by applying assigned key policy encoding to provide flexible access control over seven fundamental operations (e.g. addition, removal, etc.) from ciphertext.

SECURITY ANALYSIS

This paper is in many ways quite similar to our prior work. The security of all systems in this article depends in this situation on HRES' semantic safety and in ABE. We employ both the attack model and the security model to prove the security of our system. Four without honest adversaries verify this claim. The Authorized is not exempt from this; all other entities may be corrupted. That is why we built four simulators (Sim_{DP}, Sim_{DSP}, Sim_{CP}, Sim_{DR}) to battle their enemies (A_{DP}, A_{DSP}, A_{CP}, A_{DR}). In the event of semi-honest opponents, Scheme 1 can recover the quotient from encrypted data by collaborating between two DSP and CP servers. (A_{DP}, A_{DSP}, A_{CP}, A_{DR}). Sim_{DP} simulates A_{DP}: Sim_{DP} only needs to outsource the data is by calling $EncTK(m_i,PK)$, Therefore the safety may be inherited straight from the original HRES. Although DP may match one server (for example, DSP), A_{DSP} can only get the partial decryption result $[m_i]_{pkCP}$ through $PDec1([m_i],sk_{DSP})$ in Step 3. Finally, A_{DP} can get the ciphertext $[m_i]_{pkCP}$ and [mi]. Owing to the security of HRES, A_{DP} Could not obtain anything outsourced from the data from other users.

CONCLUSIONS

We present four privacy-preserving division algorithms that can support both encrypted fixed-point numbers and fractional numbers, and which can be modified to handle computations over these numbers. We conducted a full analysis of our schemes to ensure their correctness and security. We provide evidence that our proposals are correct and secure, and

demonstrate the practicality and scalability of our ideas using detailed computer simulations and comparisons with comparable projects. To grasp our approaches' efficiency and scalability , we conducted additional experiments and analyses of current work. This afforded us the opportunity to considerably enhance the set of privacy-preserving computation modalities by allowing users to include previously overlooked and critical computations - division and encryption of fractions and point numbers. By conducting additional tests in real-world circumstances, we'll show how our ideas can be put to use.

REFRENCES

1) M. Franz, B. Deiseroth, K. Hamacher, S. Jha, S. Katzenbeisser, and H. Schr¨oder, “Secure computations onnon-integer values,” in 2010 IEEE International Workshop on Information Forensics and Security, WIFS 2010, Seattle, WA, USA, December 12-15, 2010, 2010, pp. 1–6.
2) M. Dahl, C. Ning, and T. Toft, “On secure two-party integer division,” in Financial Cryptography and Data Security - 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers, 2012, pp. 164–178.
3) C. Ugwuoke, Z. Erkin, and R. L. Lagendijk, “Secure fixed-point division for homomorphically encrypted operands,” in Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018, Hamburg, Germany, August 27-30, 2018, 2018, pp. 33:1–33:10.
4) Location Privacy-Preserving Distance Computation for Spatial Crowdsourcing: Song Han;Jianhong Lin;Shuai Zhao;Guangquan Xu;Siqi Ren;Daojing He;Licheng Wang;Leyun Shi, IEEE Internet of Things Journal_2020.
5) Comments on “An Efficient Privacy-Preserving Outsourced Calculation Toolkit With Multiple Keys”: Chen Li;Wenping Ma, IEEE Transactions on Information Forensics and Security_2018.
6) An Efficient Framework for Privacy-Preserving Computations on Encrypted IoT Data: Shruthi Ramesh;Manimaran Govindarasu, IEEE Internet of Things Journal_2020.
7) LPPA: Lightweight Privacy-Preserving Authentication From Efficient Multi-Key Secure Outsourced Computation for Location-Based Services in VANETs: Jun Zhou;Zhenfu Cao;Zhan Qin;Xiaolei Dong;Kui Ren, IEEE Transactions on Information Forensics and Security_2020.
8) Lightweight Privacy-Preserving Scheme in Wi-Fi Fingerprint-Based Indoor Localization: Guanglin Zhang;Anqi Zhang;Ping Zhao;Jiaxin Sun, IEEE Systems Journal_2020.
9) An Extended Framework of Privacy-Preserving Computation With Flexible Access Control: Wenxiu Ding;Rui Hu;Zheng Yan;Xinren Qian;Robert H. Deng;Laurence T. Yang;Mianxiong Dong, IEEE Transactions on Network and Service Management_2020.
10) Privacy-Preserving Traffic Flow Prediction: A Federated Learning Approach: Yi Liu;James J. Q. Yu;Jiawen Kang;Dusit Niyato;Shuyu Zhang, IEEE Internet of Things Journal_2020.

11) Privacy-Preserving Computation Offloading for Parallel Deep Neural Networks Training: Yunlong Mao;Wenbo Hong;Heng Wang;Qun Li;Sheng Zhong, IEEE Transactions on Parallel and Distributed Systems_2021.
12) On the Privacy of Matrix Masking-Based Verifiable (Outsourced) Computation: Liang Zhao;Liqun Chen, IEEE Transactions on Cloud Computing_2020.
13) Efficient Privacy Preserving Data Collection and Computation Offloading for Fog-Assisted IoT: Siguang Chen;Xi Zhu;Haijun Zhang;Chuanxin Zhao;Geng Yang;Kun Wang, IEEE Transactions on Sustainable Computing_2020.
14) Privacy Preserving Collaborative Computing: Heterogeneous Privacy Guarantee and Efficient Incentive Mechanism: in Wang;Jianping He;Peng Cheng;Jiming Chen, IEEE Transactions on Signal Processing_2019.
15) Prospect Theoretic Analysis of Privacy-Preserving Mechanism: Guocheng Liao;Xu Chen;Jianwei Huang, IEEE/ACM Transactions on Networking_2020.
16) Privacy-Preserving Double-Projection Deep Computation Model With Crowdsourcing on Cloud for Big Data Feature Learning: Qingchen Zhang;Laurence T. Yang;Zhikui Chen;Peng Li;M. Jamal Deen, IEEE Internet of Things Journal_2018.
17) A Comment on Privacy-Preserving Scalar Product Protocols as Proposed in "SPOC": Thomas Schneider;Amos Treiber, IEEE Transactions on Parallel and Distributed Systems_2020.
18) Scalar Product Lattice Computation for Efficient Privacy-Preserving Systems: Yogachandran Rahulamathavan;Safak Dogan;Xiyu Shi;Rongxing Lu;Muttukrishnan Rajarajan;Ahmet Kondoz, IEEE Internet of Things Journal_2021.
19) Privacy-Preserving Top- k Route Computation in Indoor Environments: Dae-Ho Kim;Beakcheol Jang;Jong Wook Kim, IEEE Access_2018.
20) Toward Practical Privacy-Preserving Frequent Itemset Mining on Encrypted Cloud Data: Shuo Qiu;Boyang Wang;Ming Li;Jiqiang Liu;Yanfeng Shi, IEEE Transactions on Cloud Computing_2020.
21) Privacy-Preserving Location-Based Services Query Scheme Against Quantum Attacks: Ziyuan Hu;Shengli Liu;Kefei Chen, IEEE Transactions on Dependable and Secure Computing_2020.