STM JOURNALS

Journal of Artificial Intelligence Research & Advances
ISSN: 2395-6720 (Online)
Volume 6, Issue 2
www.stmjournals.com

Secure Outsourced Computation of Geometric Progression on Vicious Cloud

Gaurav Goel*, Tejpal Sharma, Jagbir Singh, Upinderpal Singh, Gagan Singla
Department of Computer Science & Engineering, Chandigarh Group of Colleges, College of Engineering, Mohali, Punjab, India

Abstract

Cloud computing provides environment to individual, organization and business to store their sensitive data on cloud. One can store their data on cloud due to cost factor. But sometimes, data can be lost and leaked by suspicious data owner. Individual can also use cloud for platform purposes, means cloud can also be used for computation purpose. Computation can be expensive on standalone desktop when resources are limited. In this study, approach is using secure and efficient way of using malicious cloud for linear algebra computation of geometric progression. Time complexity to run geometric progression is O(n). Proposed approach will work to compute this linear algebra computation securely and efficiently on vicious cloud.

Keywords: *Outsourcing, cloud, malicious*

****Author for Correspondence*** E-mail: gaurav.coecse@cgc.edu.in

INTRODUCTION

In the domain of computer science, cloud computing is an important template in terms of computing. The big challenge of cloud computing is security. So there is need of some security measures to protect the data from unauthorized users that is stored on the cloud. The cloud providers offered pliability and scalability which produces more and more services that farm out to the cloud. In this study, some security challenges that are produced in infrastructure-as-a-service cloud environment will be discussed. Now cloud becomes highly homogeneous, so it is the first target for the attackers; as the attackers know the places from where they can find the profitable information. As a consequence, the major engineering challenge is viewed as the cloud security [1].

Nowadays malware threat scenario is quickly transforming. Malware is becoming more cosmopolitan. For governments, enterprises and end-users, the detection of malware threat is the topmost choice for them. They are trying to get more knowledge about how to detect and avoid the attacks [2–4]. For analysis and detection of these attacks, some dynamic malware tools have become more popular [5–7]. The detection of attacks accurately, malware analysis and collection of evidence depends upon the selected information sources and different monitoring mechanisms. Therefore, gathering information in detail occur higher runtime cost. An intractable tradeoff is to be produced between performance effects on analysis cost, quality of the collected data and a production system. The collected data inside a virtual machine is easy target for the attackers to change it.

RELATED WORK

Farajallah *et al*. proposed a secure one way hash algorithm which computes matrix multiplication result on server [8]. The authors provided invertible matrix and multiplied this matrix with a string which also converted into column vector form. The reciever computes the result with the same hash algorithm, which had been used by the client side. Kumar *et al*. proposed outsourcing algorithm for matrix chain multiplication over malicious server [9]. Complexity of MCM is O(n3) but when it is computed on cloud, it complexity improves by O(n2). Concept of computation, transformation, retransformation and verifiable had been used by author for computation of results. Acharya *et al*. proposed a modified hill cipher technique for non-invertible matrix [10].

In original hill cipher technique, sometimes invertible matrix did not provide accurate result. In modified approach, different encryption key was used for different matrices. Hu *et al*. proposed an algorithm to find characterstics polynomial and eigenvalue for matrix [11]. In this approach, the authors sent matrices on cloud by securing it with some parameters and decrypted it after calculating its value on client side. The authors worked on correctness of result on serve side, provided soundness for to result integrity, privacy of input and output on cloud and verifiability of result after receiving result form server end.

GEOMETRIC PROGRESSION

A geometric progression, also called geometric sequence, is collection of numbers where each term after the initial number is found by multiplying the previous one by a fixed, non-zero number called the common ratio. For example, the sequence 2, 8, 32, 128, ... is a geometric progression with common ratio 4.

Examples of a geometric sequence are powers r^k of a fixed number r, such as 2^k and 3^k. The general form of a geometric sequence is:
Where $r \neq 0$ is the common ratio and a is a scale factor, equal to the sequence's start value.

The n-th term of a geometric sequence with initial value a and common ratio *r* is given by:
$a_n = a\, r^{n-1}$

Such a geometric sequence also follows the recursive relation:
$a_n = r a_{n-1}$
for every integer n>=1

Generally, to check whether a given sequence is geometric, one simply checks whether successive entries in the sequence all have the same ratio.

Geometric Series

A geometric series is the sum of the numbers in a geometric progression. For example:
=1+3+9
$=1+1\times3+1\times3^2$
Letting *a* be the first term (here 2), n be the number of terms (here 4), and *r* be the constant that each term is multiplied by to get the next term (here 4), the sum is given by:

$$\frac{a(1-r^n)}{1-r}$$

In the example above, this gives:
=1+3+9
$=1(1–3^3)/(1–3)$
=–26/–2
=13
Here sum of numbers is 13 for given example.

PROPOSED APPROACH

In proposed approach, the authors propose to calculate geometric series on cloud and assuming cloud is malicious.

Authors have given example of geometric series of computing sum of 3 numbers which was 13 in our example. But in proposed approach we are computing:
n=Number of elements in geometric series.

Instead of computing sum from geometric series, proposed approach will work on to compute n, number of elements in geometric series on malicious cloud.

$$n=\log_r[s(r-1)+1]$$

In the proposed approach, authors are providing a formula to compute number of elements on cloud from geometric series in place of sum of geometric series.

In the above formula:
n=Number of elements in geometric series,
r=Common ratio in geometric series, and
s=Sum of geometric series.

In the proposed approach, factor r and s will be input from client and cloud will provide n after secure computation. Key generation is a used technique in proposed approach to secure computation from malicious cloud. Transformation provides alteration of proposed computation by adding some suitable factors. Retransformation involved computed geometric series result on cloud (Figure 1). This approach is used to verify the actual result and result will be received from cloud. If received result is not retransformed into original result, then it will be aborted otherwise accepted.

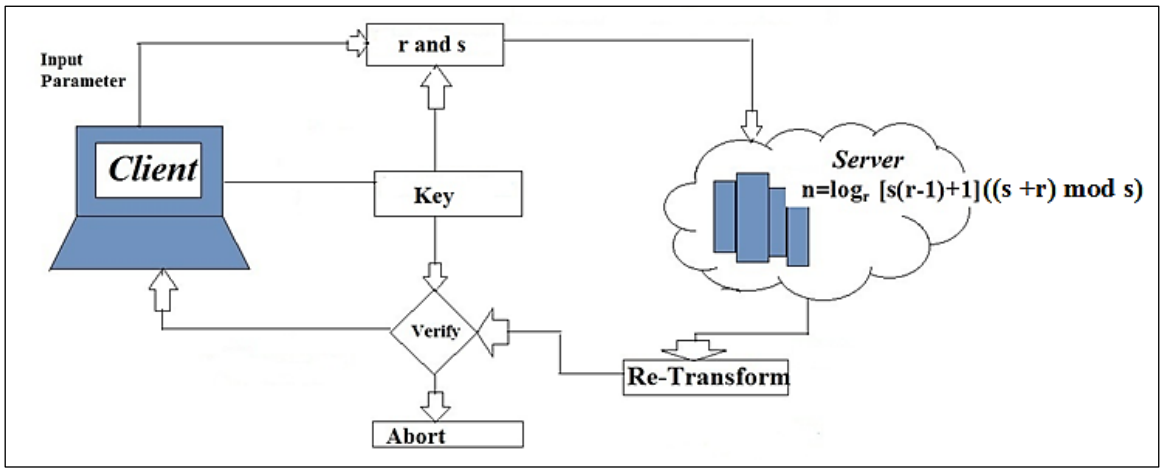

Fig. 1: *System Model to Calculate Geometric Progression.*

In Figure 1, authors proposed a mechanism to calculate number of elements available in geometric series by using formula $n=\log_r[s(r-1)+1]$. It is expected in our approach that cloud is malicious, so for securing our computation, authors have multiplied above mechanism with ((s+r)mod s).

Discussing our technique with example will provide understanding on our technique.

Given Geometric series=1+3+9 (1)

$n=\log_r[s(r-1)+1]$

Given value of s and r are 13 and 3.

$=\log_3[13(3-1)+1]$

$=\log_3[13(2)+1]$

$=\log_3[26+1]$

$=\log_3[27]$ Here value of $\log_3[27]=3$

$=3$

Number of Elements Available in Geometric Series is '3' according to Eq. (1).

Proposed approach depends upon mechanism of Key Generation, Computation, Transformation and Retransformation and Verifiability.

- **Key Generation:** Key generation is a technique to secure computation from malicious cloud. In the proposed approached, $n=\log_r[s(r-1)+1]$ is secured with ((s+r) mod s). So that actual computation cannot be leaked.
- **Transformation:** Transformation provides alteration of proposed computation by adding $n=\log_r[s(r-1)+1]$ ((s+r) mod s). On the basis of our above discussion, our proposed approach gives the result '3' according to geometric series (Number of elements). But when we calculate it with encrypted technique, it will provide some different results.
- **Computation:** Computation involved computing geometric series result on cloud. In Proposed approach, it is $n=\log_r[s(r-1)+1]$ ((s+r) mod s).

  $=\log_3[13(3-1)+1]((13+3) \text{ mod } 13)$

  $=\log_3[13(2)+1](16 \text{ mod } 13)$

  $=\log_3[26+1](3)$ [Value of 16 mod 13 is 3]

  $=\log_3[27](3)$

  Here value of $\log_3[27]=3$

  $=3\times3$

  $=9$

  Value of Proposed Computation Transformed to 9 from 3.
- **Re-transformation:** This technique used after result of computation will receive from cloud end. Re-transformation will be used by client to compute result of cloud side result into actual result.

  $=\log_r[s(r-1)+1]((s+r) \text{ mod } s)/((s \text{ mod } s+r \text{ mod } s) \text{ mod } s)$.

  $=\log_3[13(3-1)+1]((13+3) \text{ mod } 13)/((13 \text{ mod } 13+3 \text{ mod } 13) \text{ mod } 13)$

  $=\log_3[13(2)+1](16 \text{ mod } 13)/((0+3) \text{ mod} 13)$

  $=\log_3[26+1](3)/(3 \text{ mod } 13)$

  $=\log_3[27](3)/(3)$

  $=9/3$

  $=3$ (Required result).
- **Verify:** This approach is used to verify the actual result and result will be received from cloud. If received result is not retransformed into original result, then it will be aborted, otherwise accepted.

$=\log_r[s(r-1)+1]((s+r) \text{ mods})/((s \text{ mod } s+r \text{ mod } s) \text{ mod } s)$
$=\log_r[s(r-1)+1]((s \text{ mod } s+r \text{ mod } s) \text{ mod } s)/((s \text{ mod } s+r \text{ mod } s) \text{ mod } s)$
$n=\log_r[s(r-1)+1]$ (Actual Result Proved).

CONCLUSION AND FUTURE SCOPE

Proposed approach can be used for computation of geometric series result on cloud, which can be used to compute number of elements in geometric series. Since, geometric progression provided sum of geometric series. Proposed approach is working correctly to provide number of elements available in the geometric series. Proposed approach is tested on parameters of transformation, computation, retransformation and verification. Proposed technique is an outsourcing technique, in which result is computed on cloud for resource limited environment. In future this technique can be implemented on cloud to reduce complexity of geometric progression complexity and for improving efficiency of proposed system.

REFERENCES

1. Mather T, Kumaraswamy S, Latif S. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly Media, Inc.; 2009.
2. Franklin J, Perrig A, Paxson V, *et al.* An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. In *ACM conference on Computer and Communications Security*. Oct 2007; 375–388p.
3. Radianti J. Eliciting Information on the Vulnerability Black Market from Interviews. In *2010 Fourth International Conference on Emerging Security Information, Systems and Technologies*, IEEE. Jul 2010; 154–159p.
4. Zhuge J, Holz T, Song C, *et al.* Studying Malicious Websites and the Underground Economy on the Chinese Web. In *Managing Information Risk and the Economics of Security*, Springer, US. 2009; 225–244p.
5. Dinaburg A, Royal P, Sharif M, *et al*. Ether: Malware Analysis via Hardware Virtualization Extensions. In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, ACM. Oct 2008; 51–62p.
6. Anubis. http:// anubis.iseclab.org.
7. Willems C, Holz T, Freiling F. Toward Automated Dynamic Malware Analysis Using Cwsandbox. *IEEE Security and Privacy*. 2007; 5(2): 32–39p.
8. Farajallah M, Abu Taha M, Tahboub R. A Practical One Way Hash Algorithm Based on Matrix Multiplication. *Int J Comput Appl*. 2011; 23(2): 34–38p.
9. Kumar M, Vardhan M. Data Confidentiality and Integrity Preserving Outsourcing Algorithm for Matrix Chain Multiplication over Malicious Cloud Server. *J Intell Fuzzy Syst*. 2018; 34: 1251–1263p.
10. Acharya B, Rath GS, Patra SK. Novel Modified Hill Cipher Algorithm. *Int Conf Emerg Technol Appl Eng Technol Sci.* 2008; 126–130p.
11. Hu X, Tang C. Secure Outsourced Computation of the Characteristic Polynomial and Eigenvalues of Matrix. *J Cloud Comput.* 2015; 4–9p.

Cite this Article
Gaurav Goel, Tejpal Sharma, Jagbir Singh, Upinderpal Singh, Gagan Singla. Secure Outsourced Computation of Geometric Progression on Vicious Cloud. *Journal of Artificial Intelligence Research & Advances*. 2019; 6(2): 88–91p.

