SEGMENT STATURE HASH TABLE BASED COST EFFICIENT DATA SHARING IN CLOUD ENVIRONMENT

K. Karthika Lekshmi[1], Dr. M. Vigilsonprem[2]

[1] Assistant Professor, Department of Information Technology, Cape Institute of Technology

[2] Professor, Department of Computer Science and Engineering, R.M.D. Engineering College

ABSTRACT

Data sharing for dynamic groups is a promising approach that anonymously shares the data with others. Though, anonymity and traceability for sharing the data was provided in cloud environments, storage overhead with integrity and encryption computation cost remained constant. In this work, a framework called Cryptographic Multi-linear Data Sharing for Dynamic Group (CMDS-DG) is addressed to reduce the storage overhead, encryption computation cost and to maintain privacy on adding new users in a cloud environment. The cryptographic based data sharing on dynamic cloud service use RepeatKeyRotate Encryption to maintain higher privacy level. The performance results show that the CMDS-DG framework can significantly reduce the encryption computation cost by minimizing the storage overhead and maintains a higher privacy level with other data sharing methods.

Keywords*: *CMDS-DG, SSHT, Multi-linear Data Sharing

I. INTRODUCTION

A Cloud [9] is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers. Types of the cloud model include public, private, community and hybrid clouds [4]. The characteristics provided by the cloud computing include independent resource pooling, on-demand self-service, elasticity, pay-per-use, virtualization, increased storage and trust worthy metering service, etc.. To implement these features; cloud computing systems offer services at various levels, from the bottom layer to the top layer. Infrastructure-as-a-Service (IaaS) is offered in the bottom layer, which delivers services in the forms of storage, network, and computational capability. Platform as a Service (PaaS) is the middle layer which delivers services in the form of environment for software execution. Software as a Service (SaaS) locates in the top layer, which offers software applications as a service. In general, cloud computing is built over the three minimum level technologies, which includes web applications and web services, virtualization techniques for both hardware and software, cryptographic techniques for data security.

The remaining part of this paper is organized as follows. In Section II, security related works while sharing the data had been presented. Then, Section III discusses the Structural framework of Cryptographic Multi-linear Data Sharing for Dynamic Group (CMDS-DG). Impact of encryption computation cost and storage overhead are given in Section IV. Finally, the conclusion is given in section V.

II. RELATED WORKS

With the incredible data and resource sharing in a cloud environment, both cloud owners and cloud users enjoy lower marginal cost than ever before. A secure multi-owner data sharing, called, Mona [1] was designed with the objective of providing security considering storage overhead and encryption computation cost. However, storage overhead with integrity and encryption computation cost remained constant. In Oruta [2], data sharing by preserving the privacy of data were provided using a third party auditor (TPA) without retrieving the entire file. But, it did not provide mechanisms to maintain privacy while adding new users into the cloud environment. Another secure sharing approach was provided in CyberLiveApp [3] with the objective of providing privacy to the shared data. Two main advantages of using CyberLivApp were ensuring application sharing and migration between Virtual Machines. However, flexible collaboration was not provided. Role Based Access Control (RBAC) mechanism [5] was introduced with the objective of increasing anonymity and improving user revocation through algebraic structure. However, a collaborative framework was not ensured. A dynamic audit service model was introduced in the paper [6] with the aid of an index - hash table and random sampling with the motive of reducing computation and storage overhead. But, scalability remained unsolved. In paper [7] auditing of data stored in a dynamic manner was addressed using index-hash table mechanism. Another method was designed in [8] against unauthorized access by integrating user behavior profile and decoy technology. Many existing issues still need refinements, including, cost of cryptographic operations, storage overhead, privacy-preserving access control etc. In the proposed work, a framework called Cryptographic Multi-linear Data Sharing for Dynamic Group (CMDS-DG) is presented. This framework handles multiple owners in the dynamic cloud environment.

III. Structural framework of Cryptographic Multi-Linear Data Sharing for Dynamic Group (CMDS-DG)

The structural framework of CMDS-DG is shown in Figure1. This framework includes three stages, namely Crytographic Multi-linear Mapping, construction of Segment Stature Hash Table and Crptographic based Data Sharing between cloud users.

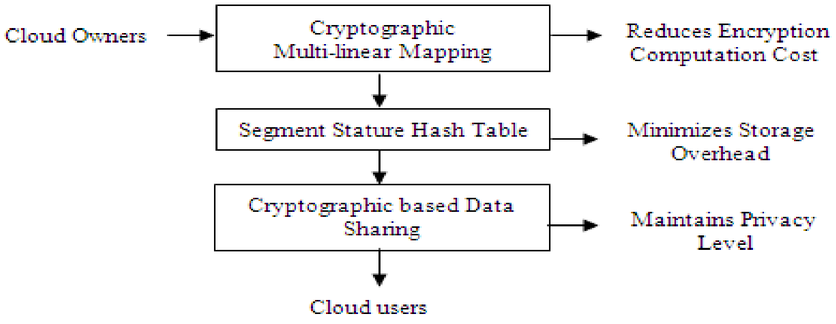
Cloud Owners
Cryptographic Multi-linear Mapping
Reduces Encryption Computation Cost
Segment Stature Hash Table
Minimizes Storage Overhead
Cryptographic based Data Sharing
Maintains Privacy Level
Cloud users

Figure 1. Framework of CMDS-DG

Two parameters Group operations and Mapping key are obtained in the proposed framework. Furthermore, the proposed framework uses a Hash based mechanism called Segment Stature Hash Table during data sharing in a cloud environment. The elaborate description of each stage is explained in detail in the following sections.

3.1 Cryptographic Multi-linear Mapping

The framework CMDS-DG provides a Cryptographic Multi-linear Mapping to ensure that security is provided with minimized encryption computation cost. When compared to the conventional cryptographic bilinear mapping that offers pairing between two cloud users, the cryptographic multi-linear mapping ensures data sharing between multi-owners and many cloud users.

Let us assume the cloud owners as '$CO_1, CO_2, \ldots . CO_n$' of order '$p$' with cloud service provider 'CSP_1', then Cryptographic Multi-linear Mapping is formalized as

$$CO_a * CO_b \rightarrow CO_{a+b} \quad for \ (a+b) \leq n \qquad 1$$

Where a, b are two different cloud owners, which contains dissimilar files or data, n represents the number of data or file contained by the cloud owners.

From (1) group operations between cloud owners 'CO_a' and 'CO_b' is performed in an efficient manner. Let us assume that '$p, q \in CO_i$' then '$sum(func, i, p, q)$' measures '$p + q \in CO_i$' whereas '$sub(func, i, p, q)$'measures '$p - q \in CO_i$'. Here p and q are data retrieved from a particular cloud owner.To share data between four cloud users 'CU_1, CU_2, CU_3, CU_4, they form the group a, b, c, d and broadcast $G_1^a, G_2^b, G_3^c, G_4^d$ using the mapping key.

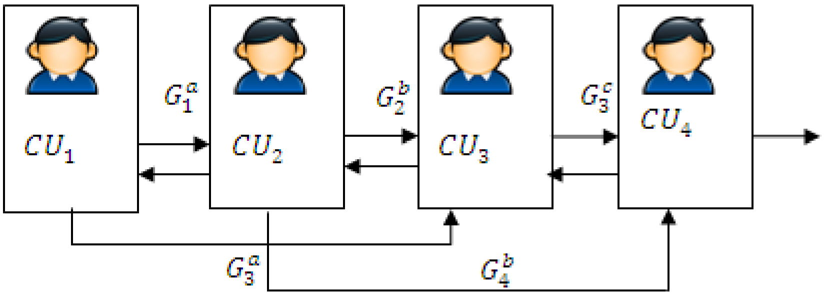

Figure 2. Design of Cryptographic Multi-linear Mapping

The mapping key for data sharing between 'G_1, G_2' and 'G_3, G_4' is formalized as given below

$$MK_{1,2} = (G_1, G_2) = G_1^a \qquad 2$$

$$MK_{2,4} = (G_2, G_4) = G_2^b \qquad 3$$

Where a, b, c and d are group names**.** As illustrated in the above figure 2, data sharing between cloud users are performed through mapping key 'MK'.

3.2 Segment Stature Hash Table (SSHT)

Once efficient data sharing between multi-users are performed, efficient handling of storage has to be performed to reduce the storage overhead. The objective behind the application of Segment Stature Hash Table is the efficient mapping of each key to only one hash value. Due to this, multi-linear mapping is efficiently performed by applying Segment Stature Hash Table. In addition, the storage overhead during data sharing is also reduced because only the encrypted file is shared with others.

The Segment Stature Hash Table consists of a table with three fields, namely Cloud Owner ID no, Group Value, Mapping Key generated for each cloud user.

Table 1. Segment Stature Hash Table

Content	**Description**
CO_ID	Cloud Owner ID no (CO_1, CO_2, CO_3, CO_4) and so on
G_V	Group Value $(G_1^a, G_2^b, G_3^c, G_4^d)$ and so on
M_Key	Mapping Key generated for each cloud user $MK_{1,2}$, $MK_{3,4}$ and so onk

3.3 Cryptographic Based Data Sharing

Cryptographic based data sharing is performed using RepeatKeyRotate Encryption Algorithm. The algorithmic steps are listed below

```
//Algorithm – RepeatKeyRotate Encryption
 Input: Cloud Owner ID No, Group Value, File
 Output: File sharing between multiple owners.
 Initialize the cloud owner with file to be sent
     Let the cloud owner ID No be ‘$CO_i$’
     Let the file to be sent by ‘$CO_i$’ be ‘$File_i$’
 For all $CO - ID_i$
     For all $G - V_i$
         Generate mapping key $M - Key_i$ for data sharing using (4)
         Encypted file $EFile_i$ = ($M – Key_i$ | $File_i$)
         Encypted file $EFile_i$ is shared between multi-owners
     End For
 End For
```

As given in the algorithm, initially, the cloud owner who wants to share the file or data with others is initialized with the Cloud Owner ID no and Group Value. The generated Mapping Key for each cloud users from SSHT is also extracted. Based on the mapping key for each cloud owner, encryption is performed with the motive of reducing the storage overhead. By obtaining separate keys for each cloud owner, higher amount of privacy is maintained.

IV. EXPERIMENTAL SETUP

The proposed framework is tested and the outcome is discussed in this section. Extensive simulations using Cloudsim are conducted to measure and evaluate the efficiency of the proposed framework. Based on the results, the impacts of two parameters, namely, encryption computation cost and storage overhead are illustrated. Each instance type is configured with a specific amount of memory, CPUs, and local storage. This type is equipped with two quad core 2.33-2.66 GHz Xeon processors (8 cores total), 7 GB RAM, and 1690 GB local disk storage.

Cryptographic Multi-linear Data Sharing for Dynamic Group is compared with the existing Multi-Owner Data Sharing for Dynamic Groups in the Cloud (MONA) [1] and Privacy-Preserving Public Auditing for Shared Data in the Cloud (ORUTA) [2].

4.1 Impact of Privacy

In table 2 we compare the privacy of the proposed framework using the RepeatKeyRotate Encryption on multi-owner data sharing. The experiments were conducted using varied number of cloud owners and cloud users, which is measured in terms of percentage (%).

Privacy (%) = (Data Retrieved by cloud users (KB) / Data Requested by cloud user (KB)) * 100

Methods	Privacy (%)
Mona	61
Oruta	70
CMDS-DG	77

Table 2 Tabulation for Privacy

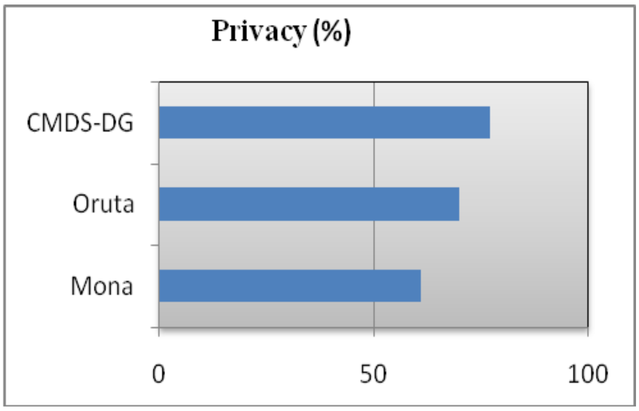

Figure3. Measure of Privacy

To explore the influence of privacy rate on CMDS-DG framework, the experiments were performed by applying 35 different cloud owners and 21 different cloud users from six different sequences obtained from allbookstores.com as depicted in figure3. The figure shows that the privacy reaches its zenith compared to two other methods because of the application of cryptographic based data sharing using a RepeatKeyRotate encryption algorithm. The application of the RepeatKeyRotate encryption algorithm efficiently extracts each key for different users which help in improving the privacy measure by 12.82 % when compared to Mona [1] and 6.41% when compared to Oruta [2] respectively.

4.2 Impact of Data Sharing Delivery Ratio

Finally, table 3 provides the data sharing delivery ratio of CMDS-DG framework for seven different cloud owners that is measured in terms of percentage (%). The Data sharing delivery ratio using CMDS-DG is the percentage ratio of data received by cloud users to the data sent by the cloud owners.

$$DSDR = \frac{Data\ received\ by\ cloud\ users\ (KB)}{Data\ sent\ by\ cloud\ owners\ (KB)} * 100$$

The data sharing delivery ratio between the 35 cloud owners and 21 cloud users for efficient data sharing in cloud environment is shown in Figure4. It shows that the proposed CMDS-DG framework potentially yields better results than existing Mona [1] and Oruta [2].

No. of cloud owners	**Data sharing delivery ratio (%)**		
	CMDS-DG	**Mona**	**Oruta**
5	80	70	60
10	83.3	75.25	69.23
15	85	80.13	71.43
20	75	68.35	62.36
25	72.8	65.22	55.19
30	74.55	69.13	61.32
35	80.25	72.33	64.81

Table 3 Tabulation of Data Sharing Delivery Ratio

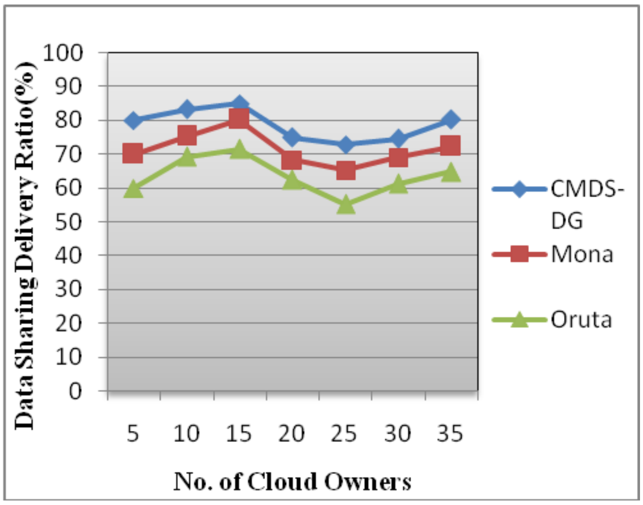

Figure4. Data Sharing Delivery Ratio (%)

The CMDS-DG framework increases the data sharing delivery ratio between the cloud users and cloud owners by 5 – 12 % compared to Mona [1] and is improved by 15 – 25 % compared to Oruta [2].

V. CONCLUSION

In this work, a framework called, Cryptographic Multi-linear Data Sharing for Dynamic Group (CMDS-DG) is addressed to minimize the encryption computation cost and to reduce the storage overhead during data sharing between multiple cloud owners and cloud users. This work shows how encryption computation cost is reduced using the Cryptographic Multi-linear Mapping. It also shows how the storage overhead is reduced using Segment Stature Hash Table. We further show attainable performance gains of the proposed framework in terms of privacy and data sharing delivery ratio by applying RepeatKeyRotate Encryption. Performance results show that the proposed CMDS-DG framework provides comparatively better efficiency in terms of privacy and data sharing delivery ratio compared to state-of-art works.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Member, Boyang Wang, and Jingbo Yan, “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,” IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 6, June 2013.

[2] Boyang Wang, Baochun Li, and Hui Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,” IEEE Transactions on Cloud Computing, Vol: 2, Issue: 1, 2014.

[3] Jianxin Li, Yu Jia, Lu Liu, Tianyu Woa, “CyberLiveApp: A secure sharing and migration approach for live virtual desktop applications in a cloud environment,” Future Generation Computer Systems., Elsevier journal, 2013.

[4] K.KarthikaLekshmi, Dr. E. Baburaj,”Data Integrity Issues in Cloud Storage System-A Survey,” International Journal of Digital Content Technology and its Applications, Vol.8, No.3, June 2014.

[5] Yan Zhu, Gail-Joon Ahn, IEEE, Hongxin Hu, Di Ma, and Shanbiao Wang,” Role-Based Cryptosystem: A New Cryptographic RBAC System Based on Role-Key Hierarchy”, IEEE Transactions On Information Forensics And Security, Vol. 8, No. 12, December 2013.

[6] Yan Zhu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau, Ho G. An and Chang-Jun Hu," Dynamic Audit Services for Outsourced Storages in Clouds", IEEE Transactions On Services Computing, Vol. 6, No. 2, April-June 2013.

[7] Rakhi Bhardwaj, Vikas Maral," Dynamic Data Storage Auditing Services in Cloud Computing", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-2, Issue-4, April 2013.

[8] Salvatore J. Stolfo, Malek Ben Salem, Malek Ben Salem," Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud", IEEE Computer Society, Feb 2012.

[9] Rajkumar Buyya, Chee Shin Yeo and Srikumar, Venugopal, "Market-oriented cloud computing:Vision, hype, and reality for delivering IT services as computing utilities", In Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, pp. 5-13, 2008.