Mitigating the Threat due to Data Deduplication Attacks in Cloud Migration using User Layer Authentication with Light Weight Cryptography

Aruna M G, Mohan K G

Abstract: ***The widespread adoption of multi-cloud in enterprises is one of the root causes of cost-effectiveness. Cloud service providers reduce storage costs through advanced data de-duplication, which also provides vulnerabilities for attackers. Traditional approaches to authentication and data security for a single cloud need to be upgraded to be best suitable for cloud-to-cloud data migration security in order to mitigate the impact of dictionary and template attacks on authentication and data integrity, respectively. This paper proposes a scheme of user layer authentication along with lightweight cryptography. The proposed simulates its mathematical model to analyze the behavioral pattern of time-complexity of data security along with user auth protection. The performance pattern validates the model for scalability and reliability against both authentication and data integrity.***

Keywords: Cloud computing, Authentication, De-duplication, Data security, Cloud-to-Cloud data migration, Hashing, Cryptography

I. INTRODUCTION

Right from the cloud prospect to the cloud users, the security of the data is a prime concern. In 2008, a survey conducted by IDC enterprises revealed that security is the primary factor in deciding to adopt the cloud [1]. Whereas, a recent survey conducted in 2018 by IDG provides surprising statistics that today 73% organization has already adopted cloud and rest planning to adopt in the very near future [2]. Out of 73 % of organizations, 42 % use a multi-cloud strategy. This paradigm shift raises a research question, that whether there is no security risk involved with the cloud by now or the business requirement compelled the enterprises to adopt the cloud services. Off-course, there is a business compulsion for enterprises to adopt the cloud to meet the feasibility of the global economy. In contrast, the security requirements have shifted from one layer to another dimension with adopting the trend of multi-cloud tenancy that offers resilience to adopt technologies and essential service to the critical applications [3-4].

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author

Aruna M G, Associate Professor, Department of Computer Science and Engineering, M S Engineering College, Bengaluru, India.

Mohan K.G*, Professor and Head, Department of computer science and Engineering, Presidency University, Bengaluru, India.

One of the primary reasons to adopt a multi-cloud strategy is to gain the cost-saving of the storage as well as an additional backup by keeping data on the more cloud storage models [5]. But the question arises that how the cost of SaaS is minimizing to attract the existing cloud users to migrate their data to the new platform. This question is answered by understanding the mechanism of the process adopted by the cloud service provider for the data de-duplication. In order to reduce the cost of data storage scalability, the de-duplication is widely adopted for data storage management [6]. The models adopted for the data de-duplication introduces vulnerabilities that provide a way to compromise the user's data and its privacy information by means of various attacks [7-9]. This paper proposes an attack framework and a mitigation model for secure data migration from cloud to cloud. Figure 1 shows the architectural diagram of the system model.

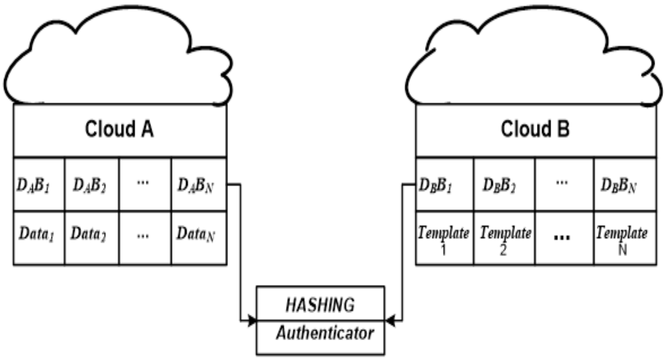

Fig.1. Architectural diagram of the of proposed secure data migration model

The proposed model constitutes of the generalized architecture of the two clouds where the cloud one bucket maintains the data and its templates into the cloud B. The trust model is built on the basis of the hash authenticator.

A. Cloud to cloud migration

The term cloud migration initially gives a sense of on premise data and system moving to the cloud infrastructure. The situations whereas already organization system and data are on the cloud, they move or migrate their storage as a Service from one vendor to another cloud vendor that makes companies to adopt multi-cloud tenancy and requirement of cloud to cloud data migration services. The cloud to cloud(C2C) Data migration services require to handle many of the complexities involved mainly to avoid speed collisions, false starts, and finally, a seamless migration with the least cost, time, and disruption. The data movement process needs to ascertain the location of the new datacenter and the bandwidth capacity.

The services to C2C migration must consider the capabilities of security, period and automatic updates, scalability as well as device independence.

B. Reason for C2C Migration

The organization adopting multi-cloud tenancy requires building logical strategy as per business factor to choose the cloud vendors.

The business factors many include security, reliability, or many other compatible features requirements. Whereas, the business process being very dynamic, the key factors itself changes accordingly over which the initial C2C migration decision is taken, and that continues a thrust of C2C migration. The few compelling requirements may include:

- A new destinated cloud may offer a performance improvement guarantee with the new system.
- The availability of additional services requires user applications, as well as a large number of APIs and integration tools.
- Price Benefit.
- Better service-level agreements and uptime
- Larger scalability to accommodate your business growth
- Decrease your DevOps and deployment timelines

These above reasons partly or fully could be the motivating factors to migrate from one cloud to another cloud or in simple word to have communication among multi-cloud tenancy environment.

C. Challenges in C2C Migration

In order to reduce the complexities for moving from on-premise to cloud infrastructure, every cloud service provider adopts their proprietary state of art close architecture. These architectures are strengthened with auto-update and maintain along with the associated requirements of hardware, operating systems, software, and storage to reduce the cost, time, and efforts require. The close architecture of cloud vendors brings synchronization issues while c2c migration. The synchronization components include seamless compatibility among operating systems, network architecture, VM configuration, databases, and many more management tools. Therefore, migrations itself is a cumbersome problem as a potential re-architecting effort is involved.

D. Decision perspective for C2C

In the decision perspective, the factors including cost, risk assessment, and overall performance and business need benefits require to be evaluated as it takes place while on-premise migration to the cloud at first instance. In a nutshell, it shall be feasible enough in multi-facet aspects of the operation, finance, and technological advantages. Yet another critical sense of decision says that to maintain a better synergy with the vendors and partners in both operational and cost aspects to manage and maintain reliable and high-performance bridges, the early decision of migration reduces the increasing complexities and challenges. This paper proposes a framework model for secure authentication using a token-based system for data deduplication layers of cloud security. The paper is organized as section II described the related work as a part of a review of literature, section III describes the proposed system model, section IV discusses the results and analysis and finally section V explains the conclusion.

II. RELATED WORK

There are different dimensions of the data in the modern edge of computing, where the Internet of things has a leading role to generate the data which requires cloud as a storage platform. Due to cloud vulnerabilities, it is necessary to protect the data generated by the IoT stored in the cloud from various data attacks, thereby maintaining the reliability of the storage by maintaining its integrity. The existing method, including RSA, poses huge computational overheads, whereas the signature-based methods do not fit suitable in the massive sensor data storage. The work of Zhu et al. (2019) proposes an algorithm based on a short signature that claims minimization of computational overhead and efficiency against a message attack. However, its dependencies for auditing on the third party does not make its reliable for secure data migration from cloud to cloud as many of the IoT application require multi-cloud infrastructure[10]. The traditional software as a service is evolving to meet the customized requirement of the users considering requirements like security in a multitenancy environment Ali et al.(2019),[11]. In the healthcare sector, the usage of the cloud to cloud(C2C) data migration is of high requirement, where the patient data are shared by the intra-cloud users. In these situations, the security requirements are at high demand to protect private information. The approach of the encryption for the attributes provides a way to protect privacy Edemacu et al. (2019) [12]. Zhang et al. (2019) presents scheme to handle the overhead of authentication with the balance of control on the un-trusted clouds using certificates and one-way authentication to achieve light-weighted mechanism [13]. The use of modified RSA, signature, encryption, and other authentication having their own limits, a new trend of use of blockchain is witnessed in many of the security paradigms. One of the works of Zuo et al. (2019) focuses on the security aspect cloud-based of medical on-demand services by overcoming traditional attribute-based encryption (ABE) to meet the challenges of both down and up-scaling of subscriptions by using blockchain along with ABE and validated it against the collusion attack [14]. The open architecture of the device brings various kind of attacks due to vulnerabilities of the device and inject to the cloud that can be controlled by the suitable device authentication methods beforehand uploading the data to the cloud. The authentication method proposed by Yanambaka et al. (2019) uses a concept of physical uncolorability by avoidance of saving of the device-related data into the cloud servers with optimal usage of keys and achieves robustness and lightweight with scalability [15]. The combined efforts of authentication of healthcare-related data with IoT based control systems ensure a secure mechanism of preserving privacy and data security on the cloud by preventing malicious access [16]. Apart from this, the privacy protection of the wearable device of the IoT ecosystem is being studied by Zhang et al. (2019), while publishing the data using distance vector mechanism [17].

With the balance between security and storage costs, the growing scale of digital medical data is being addressed through improved deduplication and ABE and minimized computing overhead. Ma et al. (2019) take up the problem of revocation of attributes while deduplication by exploiting the nature of prime number and agent key with ciphertext, where the computational overhead is reduced by means of third-party decryption [18].

The design approach by Amaral et al. (2019) assures the integrity of the data in a scalable manner to handle the tradeoff between communication and storage balances. The validation of the model takes place with an adversary model. Although, this model can handle various file types but on the non-incremental data [19]. Most of the applications, including health care and IoT based systems, generate large data periodically where the use of certificate poses additional overhead. One of the works by He et al. (2019) claims a secure data integrity scheme using a certificate less method [20]. There is a paradigm shift into the architectural layers of cloud computing to support a highly distributed deployment. The new model includes synchronization of cloud resources with the edge and fog. This brings a challenge to security requirements due to complex heterogeneity. A collaborative approach of development, security, and operation is proposed by Díaz et al. (2019) as a cybersecurity watchdog in an autonomous mode [21].

III. SYSTEM MODEL

The system model of multi-cloud architecture for cost-effective data storage is based on the assumption that due to the strong de-duplication process, the cloud can offer cost-effective data storage services so that the cloud user adopts to migrate from one cloud to another cloud. A detailed process flow of the proposed architecture of the trust mechanism used during data migration is shown in Figure 2. The data(D) is applied to the Hashing algorithm (HA) at the cloud -A(CA) and on the other side the same hashing algorithm at the cloud side (HB) if both HA is found equal to HB then it ensures the verification of integrity is true. If there is an attack that occurred on the hash function, the user needs to trust the cloud of choice to evaluate the trust factor, which is explained in the attack scenario.

A. Attack Scenario

The simple authentication process to the cloud provides a vulnerability to perform the de-duplication attack in the cloud data migration scenario. The process of the data integrity and cloud trust identifies the point of attack, and accordingly, the user decides their trust level to migrate to the particular cloud of not.

The system maintains a reference unit for every data and respective cloud hash as R_i ={R_1,R_2,R_3,…..R_A, R_B,…R_n}

Check for Integrity: $$\left.\begin{matrix} H_A = H_B \\ H_A \neq H_B \end{matrix}\right\} \begin{matrix} True \\ False \end{matrix}$$

Check for Trust: $$\left.\begin{matrix} R_A = H_A \ \text{and} \ R_A = H_A \\ R_A = H_A \ \text{and} \ R_A = H_A \end{matrix}\right\} \begin{matrix} Trust: Yes \\ Trust: No \end{matrix}$$

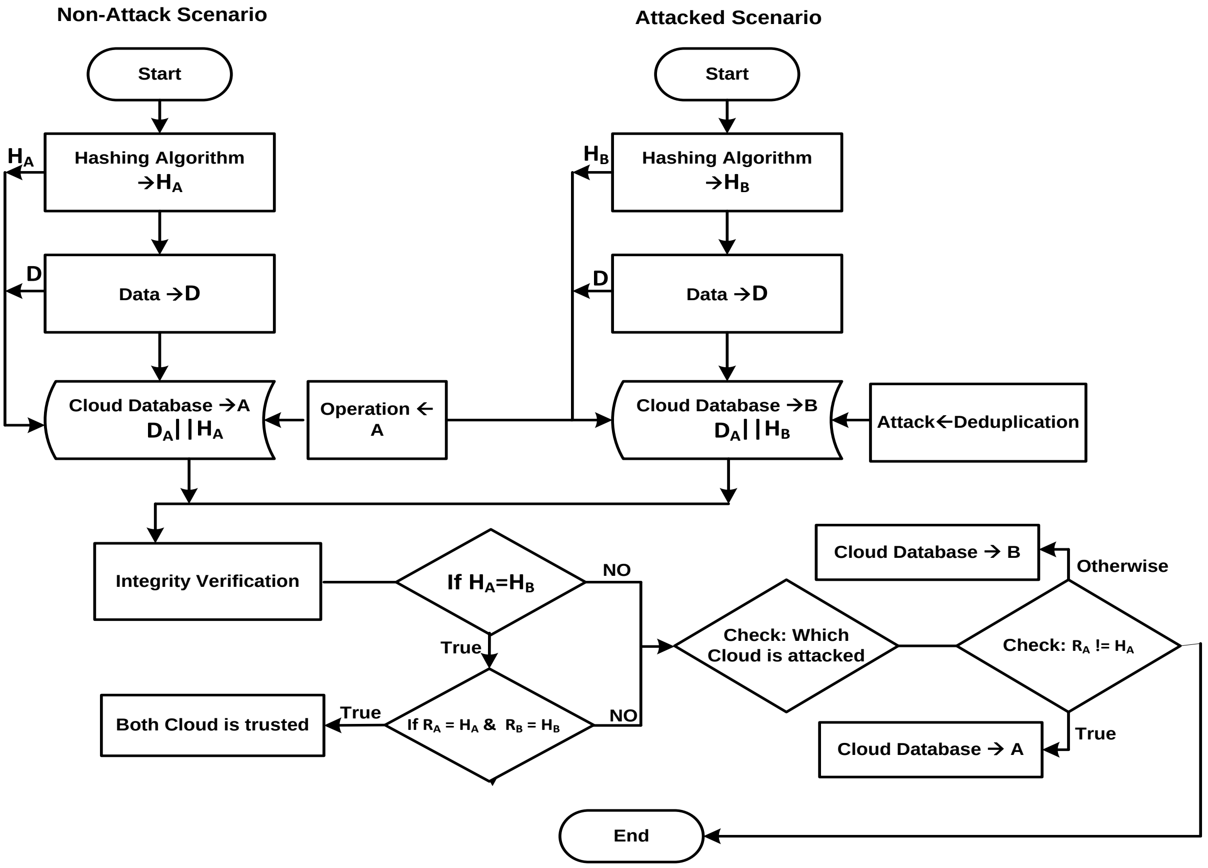

Fig.2 Process mechanism of the security model due to the threats of deduplication in data migration from C2C

B. Token Based Authentication

In the token-based authentication framework, the cloud user initial registration takes certain credentials as fn, l_n, a, e, and p, as their data uploader administrator's first-name, last-name, age, email id and the password as the first level of the authentication credentials. The combined user-authentication credential 'eAuth' vector, which is used during the data upload and deduplication process. The authenticator engine-(AE), notify the cloud user through secure-socket layers auto-generated messages for successful entry as a cloud user.

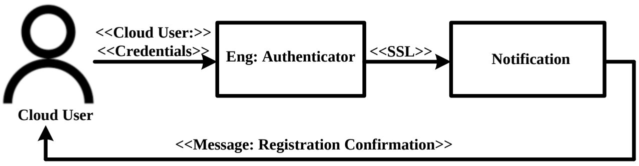

Fig.3 New cloud user registration validation

The attacker tries to get the user's credentials by some means of phishing; therefore, the framework validates the duplicate credentials and rejects the re-registration with the same user credentials. In case of dictionary attack for the user credentials and authentication token, the framework proposes a random process of matching credential of first layer Auth-code-(MCFL-AC). The algorithm for MCFL-AC is as described below:

Algorithm 1: Matching Credential of First Layer Auth-code-(MCFL-AC)

```
Input: e, $e_{sp}$, p
Output: User: rejection or move to AC2
Process:
Start
[$e_{cred}$]← e ||$e_{sp}$ and p
Initialize, $de_{cred}$,
if ($e_{cred} \neq de_{cred}$)
reject user credential
else, move to: AuthCode-2 generator
End
```

The credentials (e) is concatenated with the associated service provider for the message notification service (**e_{sp}**) that provides the e-credential of the new cloud user who has been notified by the message notification. In the same way, the cloud user personal credential key as 'p' provided during the initial registration process forms attributes for the duplicate registration as well as a first layer authentication. For the duplicate $e_{cred,}$ check a pointer: de_{cred} is flag to 0. The fig 4 shows the process flow of AuthCode-2 generation.

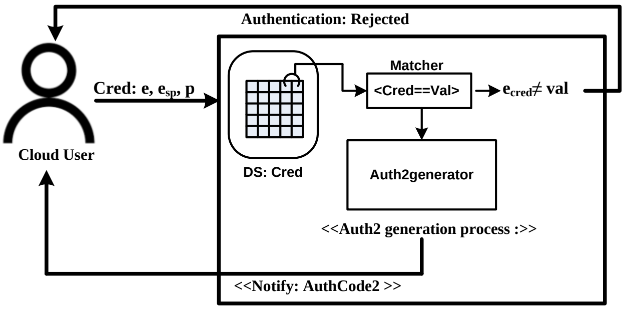

Fig.4 Authentication rejection or AuthCode2 notification

The cred:{e, e_{sp}, p } goes to the datastore (DS), where all the previously authenticated or registered cloud users credentials are stored, and performs the matching operation with its values-(val). If the cred≠val then the user first layer authentication is rejected, otherwise it moves to the operation of AuthCode-2 generation (AC2G) the algorithm of AuthCode-2 generation is described below:

Algorithm 2: Second Layer Auth-code-(AC2G)

```
Input: $S_l$, $S_h$
Output: AuthCode-2
Process:
Start
Initialize $S_l$, $S_h$
Compute:
temp AC2←Sum($S_l$, $S_h$) x $f$(rng)
AuthCode-2← Sum($S_l$, temp AC2)
End
```

In order to make the AuthCode-2 more chaotic, to seeds, namely low-value seed (Sl) and high value seed (S_h) are introduced, which can be changed periodically and randomly by the AuthCode-2 generator engine synchronized between two clouds to mitigate the effect of guessing attack. The AuthCode-2 is generated with S_l, S_h and a pseudo uniform random generator function *f*(rng) using equation (1)

$$\text{AuthCode-2} \leftarrow \sum \left\{ S_l, \left[\sum \left(S_h, S_l \right) \times f\left(rng \right) \right] \right\} \quad \text{...eq.(2)}$$

The cloud user gets authenticated at two layers and in every cycle of authentication, notified automatically as one more layer of security.

Data Upload and De-duplication: The data (D) and de-duplicated data (DeD) holds their respective timestamp in the format of a template shown in the table 1.

Table.1 Data and De-duplicated data storage format

Header-1	Header-2	Header-3
Cred	Timestamp (T_S)	(D/DeD)

The successive upload of 'D' is stored in the payload structure shown in the table-1. The de-duplication process checks for the unique records in the data stored and append only the additional record which is not found in the record. The process of matching and appending is shown in fig-5.

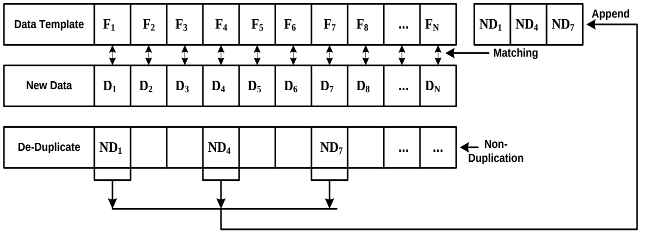

Fig.5 Matching and Appending: data template, new data, de-duplication

As the data uploads increase from the authenticated client, and efficient de-duplication process matches each block in the data store between the data template in the cloud store and each block of new data. The unique or non-duplicated blocks found during the matching operation are appended to the existing data template in the cloud store that minimizes the cost of storage. Since the data migration process among cloud-to-cloud requires on-fly encryption, therefore the computational cost of the appending, the non-duplicate data tokens should be linear with increasing data size to get a proportionate time complexity, wherewith increasing the size of data token or data file exhibits proportionate values of time as tabulated in table 2.

Table.2 Observations of time-(ms) Vs file size

Time-T(ms)	1	2.83	5.20	8	11.18
Size-(mb)	1	2	3	4	5
Time-T(ms)	14.70	18.52	22.63	27	31.62
Size-(mb)	6	7	8	9	10
Time-T(ms)	36.48	41.57	46.87	52.38	58.10
Size-(mb)	11	12	13	14	15

A filed primer (α) is initialized with a random value to evaluate the computational cost for appending non-duplicate token. For each value of the data token stack (N_r), the time (T) is computed using equation 2.

$$T \leftarrow (N_R)^A \text{ …Eq(2)}$$

The figure 6 shows the pattern of the graph between time and size for the computational cost of appending non-duplicate data token as a notion of data storage cost.

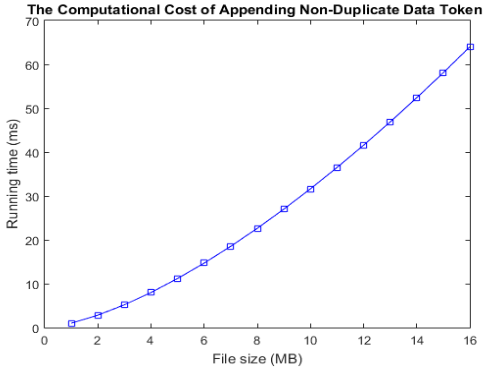

Fig.6 Computational cost of non-duplicate data token upload with varying file/token size

The section 4 describes the performance analysis of different cryptographic process on fly in detail.

IV. RESULT AND ANALYSIS

The data store of the entire user appends into the secure bucket of the respective cloud, which is modeled for the light-weight encryption with a time factor threshold with a filed primer (α) and another primer (ß) for time complexity computation for both encryption and decryption respectively. Figure 7, illustrates the performance behavior of time consistency for both encryption and decryption with varied file sizes.

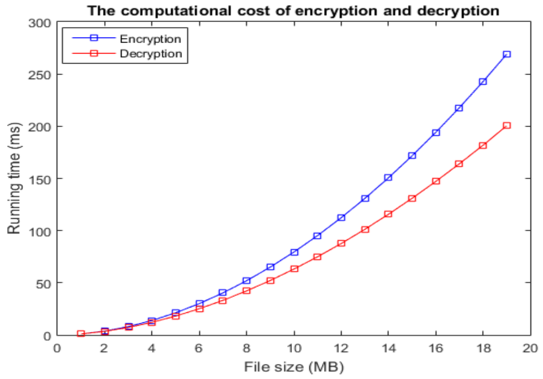

Fig.7 The computational cost of encryption and decryption: File size-(MB) vs running time (ms)

The computation of time factor takes place using equation 3 and equation 4.

$$\alpha\ [t_e] \leftarrow (u_D)^{\alpha} \text{ …equ(3)}$$
$$\text{ß}(t_d) \leftarrow (u_D)^{\text{ß}} \text{ …equ(4)}$$

The trend of both encryption time (t_e) and decryption time (t_d) for respective data (u_D) shows a proportionate and consistent incremental pattern that ensures the suitability of the cryptography system for large data sizes.

Figure 8, illustrates the computational cost of re-encryption with a key size of 256 bit for varying file sizes by computing respective computation time in milli-second.

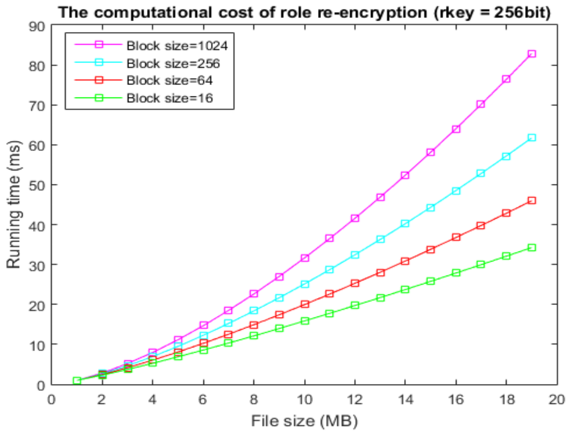

Fig.8 The computational cost of role re-encryption(rkey=256bit) for block size: 1024,256,64 and 16, File size-(MB) vs Running time(ms).

The computation of time factor for varying file size for respective block size = {1024, 256, 64, and 16} takes place using equation 5, equation, equation 7 and equation 8.

$$\alpha\ [t_{B=1024}] \leftarrow (u_D)^{\alpha} \text{ …equ(5)}$$
$$\text{ß}[t_{B=256}] \leftarrow (u_D)^{\text{ß}} \text{ …equ(6)}$$
$$\gamma[t_{B=64}] \leftarrow (u_D)^{\gamma} \text{ …equ(7)}$$
$$\theta[t_{B=16}] \leftarrow (u_D)^{\theta} \text{ …equ(8)}$$

The trend of re-encryption for varied block size(1024, 256, 64 and 16) with a key size of 256 bit shows a proportionate and consistent incremental pattern over increasing file size, that ensures fitness of the cryptography system for large data sizes. Figure 9 demonstrates the computational cost of re-encryption with a key size of 512 bit for different file size by computing respective computation time in milli-second.

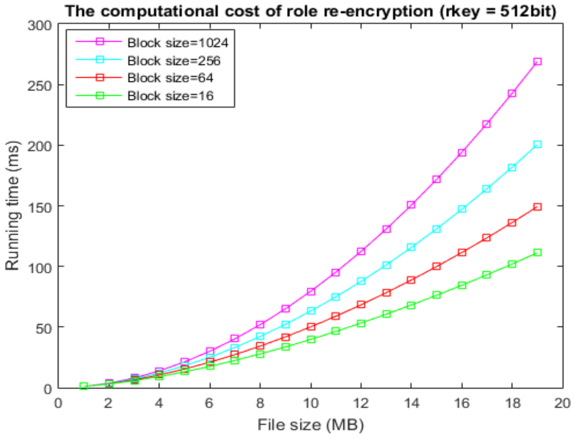

Fig.9 The computational cost of role re-encryption (rkey=512bit), of block size: 1024, 256, 64 and 16, File size-(MB) vs Running time (ms)

The computation of time factor for varying file size for respective block size = {1024, 256, 64, and 16} takes place using a similar function as demonstrated in equation 5, equation, equation 7 and equation 8. The trend of re-encryption for varied block size with a key size of 512 bit shows a proportionate and consistent incremental pattern that ensures the suitability of the cryptography system for large data sizes.

Figure 10 demonstrates the computational cost of re-encryption with a key size of 1024 bit for different file size by computing respective computation time in milli-second.

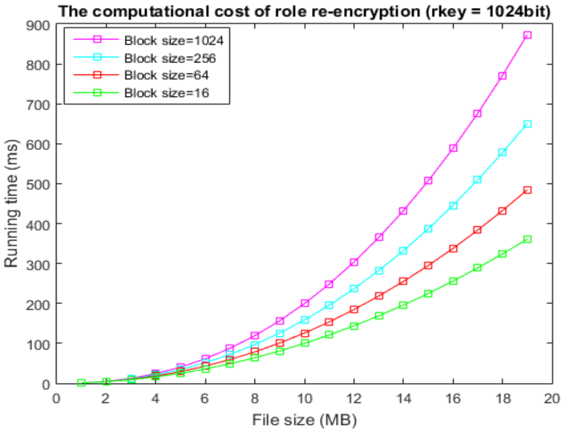

Fig.10 The computational cost of role re-encryption (rkey=1024bit), of block size: 1024, 256, 64 and 16, File size (MB) vs Running time (ms)

The computation of time factor for different file size for respective block size = {1024, 256, 64, and 16}. The trend of re-encryption for various block sizes with a key-size of 1024 bits shows a proportional and consistent incremental pattern, which confirms that the cryptographic system is appropriate for large data volumes.

Figure 11 shows the computational cost of re-decryption for varying file size for respective block size = {1024, 256, 64, and 16} by computing respective computation time in milli-second.

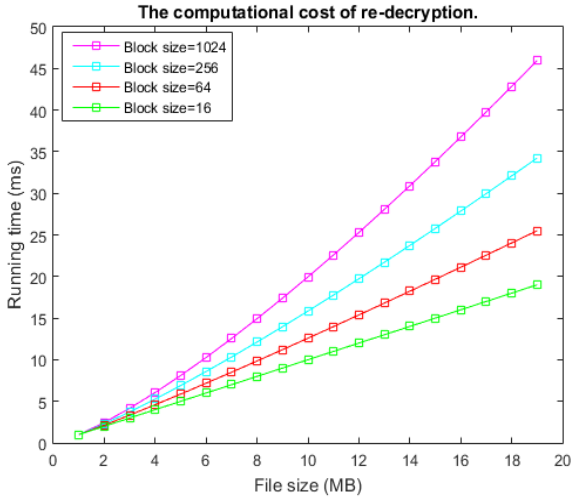

Fig.11 The computational cost of re-decryption of block size: 1024, 256, 64 and 16, File size-(MB) vs Running time(ms)

The trend of re-decryption for varied block size-(1024, 256, 64 and 16) shows proportionate, and steady performance with the incremental pattern over increasing file size, which ensures the appropriateness of the cryptography system for large data sizes.

V. CONCLUSION

The trend of data migration from cloud-to-cloud is a growing trend to meet the application requirements as well as to adopt a competitive and secure data store among the cloud service provider. The issue of authentication, along with integrity in the architecture of the eco-system of cloud-to-cloud migration, is designed. The issue of authentication is handled by providing a secure auth-token by hashing mechanism along to combat the effect of dictionary attack by the adversaries to gain authentication codes, which is one-layer advancement as compared to traditional cloud service provider authentication schemes. Another essential issue of data security against the threat of de-duplication template attack is handled by a scheme of encryption and decryption while first data incident storage and re-encryption and re-decryption for the additional unmatched data while de-duplication process. The various performance analysis for time complexity with respect to varying file size, block size, and re-keying size shows a consistent, proportionate pattern, that validates the model for scalability, interoperability, and time-complexity. The proposed system is suitable as it offers a robust and efficient mechanism and reliable to be adopted in real-time implementations.

REFERENCES

1. P. Mell, "What's Special about Cloud Security?" in *IT Professional*, vol. 14, no. 4, pp. 6-8, July-Aug. 2012. doi: 10.1109/MITP.2012.84
2. IDG Group, "2018 Cloud Computing Survey", [https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/] visited on 22nd Jan 2019
3. H. Witti, C. Ghedira-Guegan, E. Disson and K. Boukadi, "Security Governance in Multi-cloud Environment: A Systematic Mapping Study," *2016 IEEE World Congress on Services (SERVICES)*, San Francisco, CA, 2016, pp. 81-86.
4. J. Bohli, N. Gruschka, M. Jensen, L. L. Iacono and N. Marnau, "Security and Privacy-Enhancing Multicloud Architectures," in *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 212-224, July-Aug. 2013.
5. G. Liu and H. Shen, "Minimum-Cost Cloud Storage Service Across Multiple Cloud Providers," in IEEE/ACM Transactions on Networking, vol. 25, no. 4, pp. 2498-2513, Aug. 2017.
6. W. Leesakul, P. Townend and J. Xu, "Dynamic Data Deduplication in Cloud Storage," *2014 IEEE 8th International Symposium on Service Oriented System Engineering*, Oxford, 2014, pp. 320-325.
7. Shin Y, Koo D, Hur J. A survey of secure data deduplication schemes for cloud storage systems. ACM computing surveys (CSUR). 2017 Feb 6;49(4):74.
8. Li X, Shen Y, Zhang J. The verifiable secure schemes for resisting attacks in cloud deduplication services. International Journal of Grid and Utility Computing. 2016;7(3):184-9.
9. Zhao, H., Wang, L., Wang, Y. et al. J Wireless Com Network (2018) 2018: 185.
10. H. Zhu *et al*., "A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT Based on Short Signature," in *IEEE Access*, vol. 7, pp. 90036-90044, 2019.
11. A. Q. Ali, A. B. M. Sultan, A. A. A. Ghani and H. Zulzalil, "A Systematic Mapping Study on the Customization Solutions of Software as a Service Applications," in *IEEE Access*, vol. 7, pp. 88196-88217, 2019
12. K. Edemacu, H. K. Park, B. Jang and J. W. Kim, "Privacy Provision in Collaborative Ehealth With Attribute-Based Encryption: Survey, Challenges and Future Directions," in *IEEE Access*, vol. 7, pp. 89614-89636, 2019.
13. X. Zhang, C. Liu, S. Poslad and K. K. Chai, "A Provable Semi-Outsourcing Privacy Preserving Scheme for Data Transmission From IoT Devices," in *IEEE Access*, vol. 7, pp. 87169-87177, 2019.
14. R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang and Z. Wang, "Flexible and Efficient Blockchain-Based ABE Scheme With Multi-Authority for Medical on Demand in Telemedicine System," in *IEEE Access*, vol. 7, pp. 88012-88025, 2019
15. V. P. Yanambaka, S. P. Mohanty, E. Kougianos and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things," in *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388-397, Aug. 2019.

16. K. Riad, R. Hamza and H. Yan, "Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records," in *IEEE Access*, vol. 7, pp. 86384-86393, 2019.
17. Z. Zhang, B. Han, H. Chao, F. Sun, L. Uden and D. Tang, "A New Weight and Sensitivity Based Variable Maximum Distance to Average Vector Algorithm for Wearable Sensor Data Privacy Protection," in IEEE Access, vol. 7, pp. 104045-104056, 2019.
18. H. Ma, Y. Xie, J. Wang, G. Tian and Z. Liu, "Revocable Attribute-Based Encryption Scheme With Efficient Deduplication for Ehealth Systems," in *IEEE Access*, vol. 7, pp. 89205-89217, 2019.
19. D. M. Amaral, J. J. C. Gondim, R. De Oliveira Albuquerque, A. L. S. Orozco and L. J. G. Villalba, "Hy-SAIL: Hyper-Scalability, Availability and Integrity Layer for Cloud Storage Systems," in IEEE Access, vol. 7, pp. 90082-90093, 2019.
20. Y. Liao, Y. Liang, A. W. Oyewole and X. Nie, "Security Analysis of a Certificateless Provable Data Possession Scheme in Cloud," in IEEE Access, vol. 7, pp. 93259-93263, 2019.
21. J. Díaz, J. E. Pérez, M. A. Lopez-Peña, G. A. Mena and A. Yagüe, "Self-Service Cybersecurity Monitoring as Enabler for DevSecOps," in *IEEE Access*, vol. 7, pp. 100283-100295, 2019.

BIOGRAPHIES OF AUTHORS

	Mrs Aruna M G is a research scholar in Visvesvaraya Technological University, Belagavi, India. She has completed her B.E and M.Tech from Bangalore university and MGR university in 2001 and 2006 respectively. Currently, she is working as a associate professor in M S Engineering college, Bangalore, India. Her research interests is in security in cloud computing. She has overall 15 years of experience as an academician and 04 years of research experience.
	Dr. K. G. Mohan has received PhD from Anna university in 2007 in the domain of computer architecture. His area of research interest includes low power architecture design, Cloud Computing, Wireless Sensor Networks, IoT, Network Security, etc. He has overall 30 years of experience as an academician and 14 years of experience in research. He has published many international journal and conferences of repute.