JETIR.ORG | ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Security Enhancement of data within cloud using encryption mechanism

Monika Rani
Swami Sarvanand Institute of Engineering
and Technology ,Dinanagar,Punjab

Harjinder Kaur
Swami Sarvanand Institute of Engineering
and Technology,Dinanagar,Punjab

***Abstract**: Block chaining is the mechanism by which users can differently accounts within same cloud storage. The cloud environment is used in block chaining to provide the resources on shared basis. In normal situation, single user can have only one account and if other user tries to login into the system causes the chained attack. The chained attack is also known as collision. The proposed work provides the solution to this chained attack. For solving the issue, multiple tag support is provided within cloud environment. To provide the security, BLOCK CHAINING based encryption is collaborated along with multiple tag support. The proposed work provide the facility to the user for adding more records within same account using the facility of multiple tags. The collision problem is completely eliminated using the proposed work with multiple tag support. The security is enhanced since key formation is more complex as compared to mechanism without random key generation. The result of the proposed work is expressed in the form of through indicating total output, encryption time and decryption time. The result is improved by the significant margin using the proposed work that is in the range of 10% as compared to approach without multiple tag support.*

***Keywords:** Collision, Multiple tag support, cloud, BLOCK CHAINING*

Introduction

Cloud provides the users with the support in the form of resources. [1]The resources that is provided is portioned into layered forms. The layered approach includes IaaS, PaaS and SaaS. The proposed work works on the infrastructure as a service layer. This layer contains the storage-based system. The storage is mostly attacked by the hackers. The layer model of cloud is represented with the figure 1.

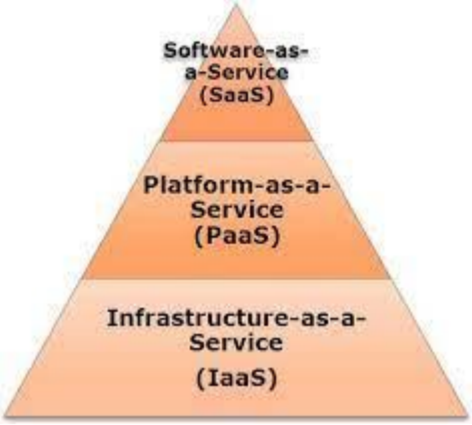
Software-as-a-Service (SaaS)
Platform-as-a-Service (PaaS)
Infrastructure-as-a-Service (IaaS)

Figure 1: Cloud Layered Model

[2]IaaS allows the users to access the storage resources as per the needs. User needs to pay for the resources that are required to be accessed. There will be service level agreement between the client and service provider. This service level agreement cannot be violated by both the parties.[3] The resource accessing can be through single user login or authorization. The authorization mechanism ensures that no unauthorized user can access the resources.

[4]During account creation and storing of data issue of collision can arise. The reason for the same is multiple users sharing the common account. [5]This cause the data to be overwritten by other user of the same account. [6]This problem is solved within the proposed system. This problem is rectified using the multiple tag support and BLOCK CHAINING encryption process. Rest of the paper is structured as under: section 2 gives the literature survey of cloud security mechanisms, section 3 gives the methodology of operation, section 4 gives the performance analysis along with result section, section 5 gives the conclusion and future scope and last section is terminated with references.

2. Review of Literature

This section presents the review of different strategies that are used to provide the security within cloud system. The cloud-based system provides the suers with the shared resources. The resources are the main point that could be hacked and to avoid the situation encryption strategies are applied.

[7] proposed a security mechanism within public cloud. The encryption is based upon the public key that is shared between the source and destination. This means that cloud security in this case is weak. The mechanism that is used is strictly based upon the RSA based mechanism. The result is expressed in the form of encryption and decryption time.

[8]proposed a binary BLOCK CHAINING encryption that is based upon the human BLOCK CHAINING encryption model. This encryption uses the private key at both the sender and receiver end. The encryption strategy that is used is secured but key generated is not complex. The collision problem however in this case is not resolved. This means that parameters can be optimized further for improving the result.

[9]proposed alarm-based strategy for handling the security within the cloud. The shared resources can be accessed with the help of accounts. The account that is common may not be suitable for this approach. Multiple tag support is missing and hence data will be overwritten in this case.

[10] proposed a format preserving encryption using the random key mechanism. The random key generates the secure mechanism and data is shared among the source and destination. The same account and multiple clients may cause the problem of collision that is not tackled through this approach. The issue is aggravated in case large volume of data is required to be stored within cloud.

[11]proposed a scalable approach for providing security within the cloud-based system. The security in this case is provided through systematic key. The key ensures better scalability and sharing of data as compared to RSA encryption-based mechanism. The throughput however is poor in this case. This can be improved through the collision resolution mechanism.

[12] proposed a trust management system within cloud computing. The cloud computing environment has multiple vendors. The reputation of the vendors allows them to sell the cloud storage. In case attack occurs, reputation within the cloud also becomes weak. To resolve the issue trust management system is implemented in this paper.

[13] proposed cloud security mechanism with DES. Data encryption standard uses the public key at source end and private key at the destination end. This means that asymmetric keys are used at the source and destination end. The mechanism also ensures that throughput is in the reasonable range. The encryption tie and decryption time in this case is high.

[14] proposed a digital signature-based mechanism to support security within cloud computing. This is one of the most secured mechanisms used within cloud. This technique ensures that unauthorized user cannot access the resources. Only issue of throughput appears within this system.

In almost all the discussed literature, collision issue is present. In addition, security is weak. This problem is rectified within t he proposed system using the collision resolution and multiple tag support based mechanism.

3. Proposed Methodology

The proposed methodology includes tag support with same index. This means that same index will be capable of storing multiple data. This is known as multiple tag support and this will remove the collision if any within t he storage system. The flow of the proposed system is given within figure 2

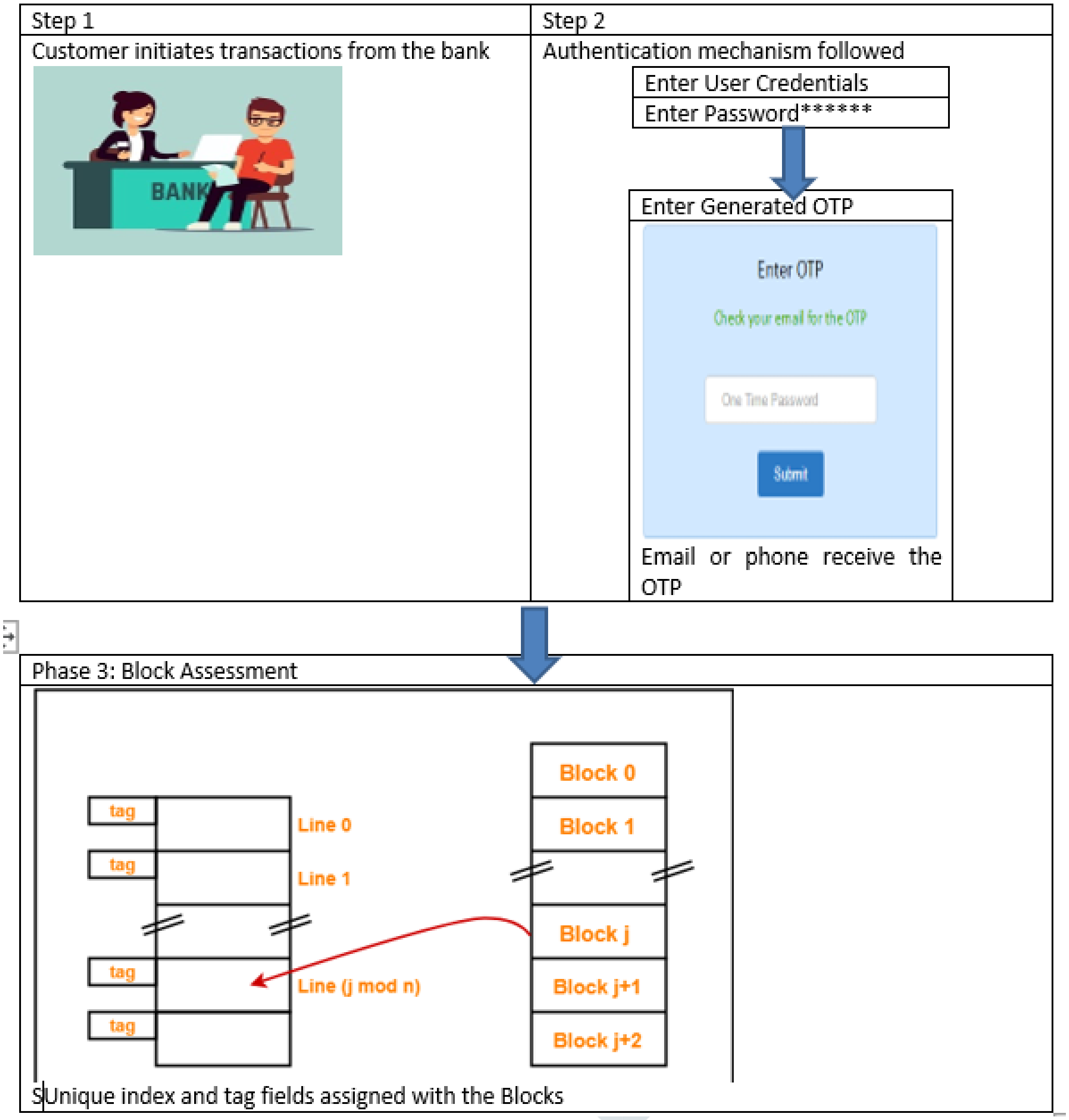
Step 1
Customer initiates transactions from the bank
BANK
Step 2
Authentication mechanism followed
Enter User Credentials
Enter Password******
Enter Generated OTP
Enter OTP
Check your email for the OTP
One Time Password
Submit
Email or phone receive the OTP
Phase 3: Block Assessment
tag
tag
tag
tag
Line 0
Line 1
Line (j mod n)
Block 0
Block 1
Block j
Block j+1
Block j+2
SUnique index and tag fields assigned with the Blocks

Figure2:Collision resolution with multiple tag support

To use the system we need to upload file onto the cloud. The file format for the usage is given in table 1

.

AC No.	Name(First)	Name(Last)	Account_Holder_Email	Gender	Ac_Group
1	Kanica	MacBarron	kbirt012@paypal.com	Female	4.9E+16
2	Nikita	Smith	narthey123@paypal.com	Female	5.6E+13
3	Ariena	Williams	aclapison212@miibeian.gov.cn	Female	3.77E+11

4	Siseley	Brown	sdummer315@miibeian.gov.cn	Female	3.57E+13
5	Spense	Johnson	smccourt454@youku.com	Male	3E+18
6	Lunus	Jones	ljasik578@prweb.com	Male	6.76E+19
7	Alfredea	Garcia	alinnit698@wisc.edu	Female	4.91E+14
8	Elvis	Lopez	atertre704@wisc.edu	Male	3.53E+12
9	Dixie	Gonzales	dtetla812@devhub.com	Female	3.56E+13
10	Aillyn	Thomas	asiddens925@weibo.com	Female	3.7E+15
11	Benet	Wilson	Blandmana876@microsoft.com	Male	3.59E+17
12	Horate	Ghidetti	Hdoogueb890@ telegraph.co.uk	Male	6.39E+19
13	Rutgerie	Joseph	Rghidettic456@microsoft.com	Male	4.51E+16
14	Vauvan	Paolazzi	Vmainstond367@ friendfeed.com	Male	6.76E+14
15	Rupci	Linnit	Rdemarse375@domainmarket.com	Male	5.49E+16
16	Fedric	Siddens	Ccasfordf432@friendfeed.com	Male	3.56E+18
17	Rodovico	Arthey	Lpaolazzig225@flickr.com paypal.com	Male	6.04E+17
18	Emog	Jackson	Emacbarronh789@flickr.com	Female	5.6E+15

Table 1: Dataset used in the proposed mechanism.

The proposed methodology that is used is given within the figure 3

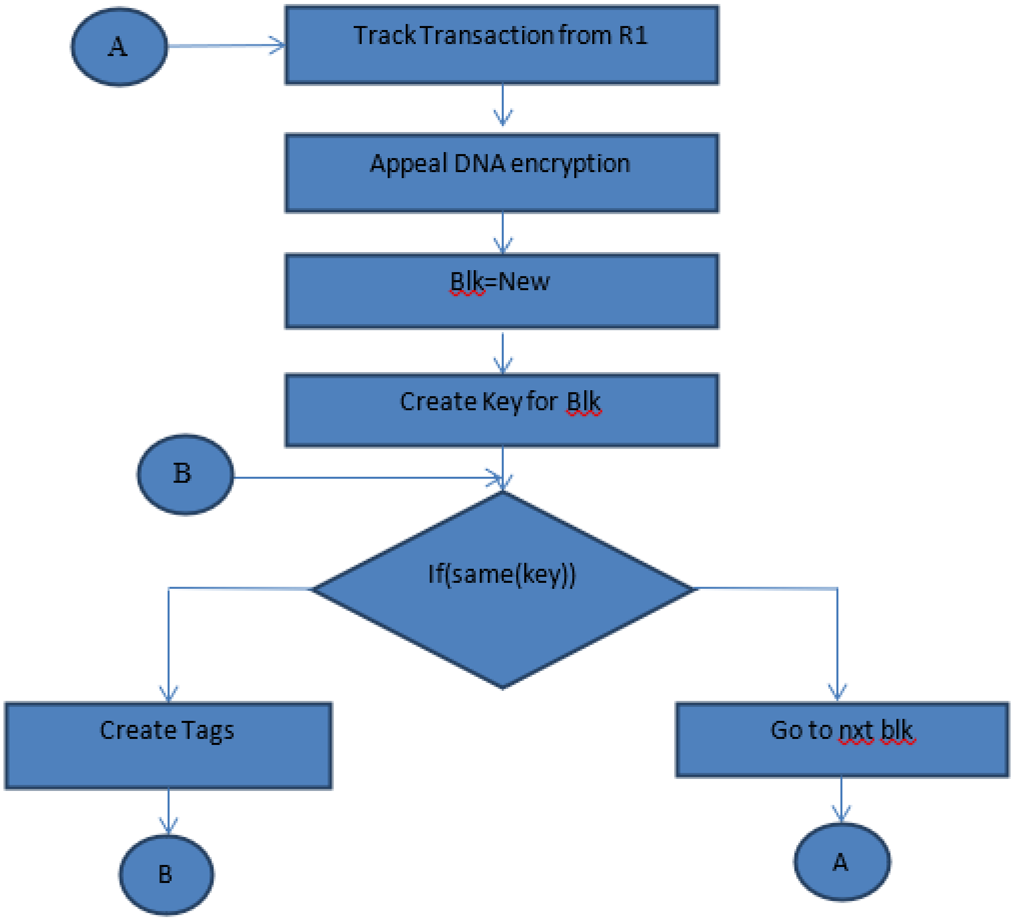

Figure 3: proposed methodology

4. Performance Analysis and result

The performance analysis indicates the result that is obtained with the proposed system. The result section also demonstrate that proposed result is better as compared to existing work. The execution time is the first metric that is demonstrated in the proposed work. The result is given within

File Size(KB)	Execution time Existing work(ms)	Execution time proposed work(ms)
500	10	5
1024	16	8
2048	22	11
4096	30	20
8192	42	25

The result is also clear within the plots. The plot for the execution time is given within the figure

Table 2: Execution time comparison

The encryption tie and decryption tie is reduced considerably using the proposed mechanism. This is given within the table 3.

File Size(KB)	Encryption and decryption time Existing work(ms)	Encryption and decryption time proposed work(ms)
500	100	5
1024	160	83
2048	202	110
4096	310	220
8192	422	250

Table 3: Encryption and decryption time comparison

The plots showing the use of encryption and decryption time is given within figure 5.

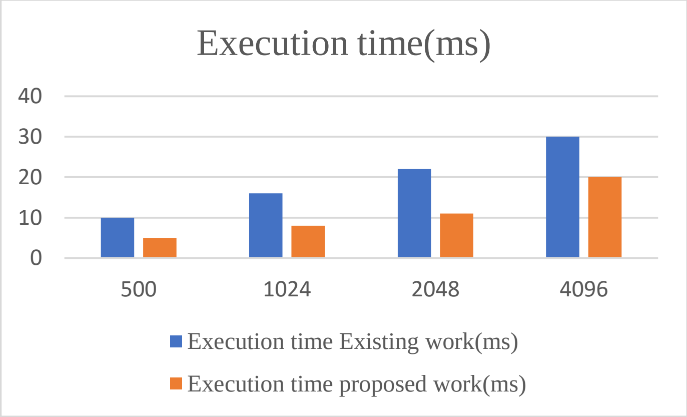

Figure 4: Execution time The encryption and decryption time is the next metric used within the proposed system.

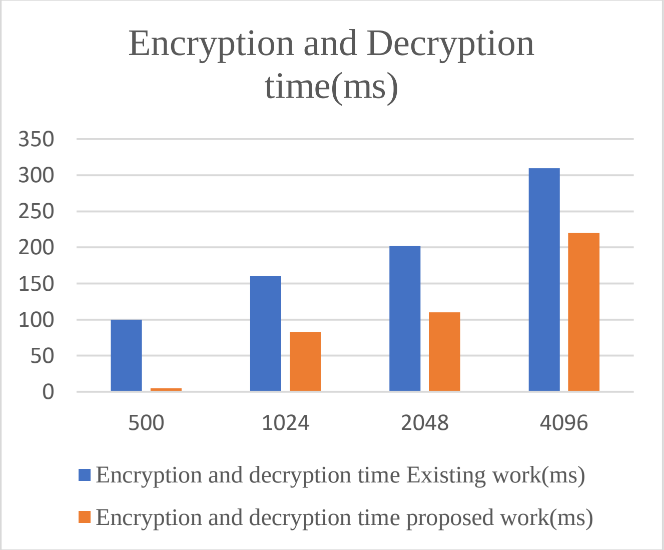

Figure 5: Encryption and Decryption time

The throughput obtained through the proposed system is also high. The throughput means total output. Since multiple tag support is present hence, throughput obtained is also high. The throughput obtained through the proposed approach is given in table 4

File Size(KB)	Throughput Existing work	Throughput proposed work
500	10.23	10.89
1024	16.123	23.45
2048	18.90	27.7
4096	20.7	28.98
8192	22.56	30.44

Table 4: Throughput through existing and proposed work

Throughput indicates the total output that is increased through the proposed approach. This is indicated with the figure 6

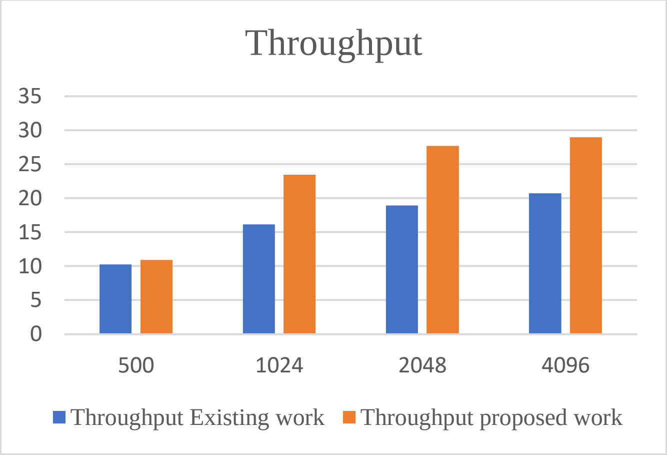

Figure 6: Throughput through existing and proposed work.

The result obtained through the existing and proposed approach indicates that proposed system is better as compared to existing approach.

5. Conclusion and future scope

The collision resolution approach employed within the proposed approach indicates that same user will be able to store data within same account. The collision will not take place and throughput will increase. The BLOCK CHAINING encryption strategy used also increases the security since private key is used at both the sender and receiver end. Multiple tag support removes the collision issue that is common in cloud environment. The service level agreement is not violated, and customer trust is also going to be increased. The encryption and decryption time is considerably reduced using the proposed mechanism. The result obtained also indicates that multiple records can be stored without collision. The random key generation ensures complex key formation. This key is shared among source and destination nodes. The key formed are complex and cannot be easily guessed. The mechanism uses the dataset that is formed offline as well as real time. The size of the dataset is limited at this time and proposed work is still required to be tested on large datasets.

This work is not yet demonstrated on the real time dataset. In future we will use real time dataset for enhancing the security of operation.

References

[1] P. Pandey, P. Dhasal, and R. Pandit, “Implementation of RSA RC5 Algorithm in Cloud,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 1, pp. 224–227, 2020, [Online]. Available: https://pdfs.semanticscholar.org/b03e/761c957820e3291232f60f239af684d33f0b.pdf.

[2] A. Zhou, Q. Sun, and J. Li, “Enhancing Reliability via Checkpointing in Cloud Computing Systems,” *IEEE*, pp. 108–117, 2021.

[3] L. M. Vaquero, “A break in the clouds: towards a cloud definition,”,” *SIGCOMM Comput. Commun. Rev.*, vol. 39, p, 2019.

[4] D. Kliazovich, P. Bouvry, and S. U. Khan, “GreenCloud : A Packet-level Simulator of Energy-aware Cloud Computing Data Centers,” *J. Supercomput.*, vol. 62, no. 3, pp. 1263–1283, 2020, doi: 10.1007/s11227-010-0504-1.

[5] C. Chen, M. Won, R. Stoleru, and G. G. X. Member, “Energy-Efficient Fault-Tolerant Data Storage & Processing in Mobile Cloud,” *IEEE*, vol. 3, no. 1, pp. 1–14, 2021, doi: 10.1109/TCC.2014.2326169.

[6] A. Dhingra and S. Paul, “A Survey of Energy Efficient Data Centres in a Cloud Computing Environment,” *IEEE*, vol. 2, no. 10, pp. 4033–4040, 2020.

[7] R. Deshmukh, “Enhanced Privacy Preservation and Data Storage Security in Public Cloud,” *Helix*, vol. 8, no. 5, pp. 3726–3730, 2018, doi: 10.29042/2018-3726-3730.

[8] M. Sohal and S. Sharma, “BBLOCK CHAINING-A BLOCK CHAINING inspired symmetric key cryptographic technique to secure cloud computing,” *J. King Saud Univ. - Comput. Inf. Sci.*, 2018, doi: 10.1016/j.jksuci.2018.09.024.

[9] Y. Meng, T. Qin, Y. Liu, and C. He, “An Effective High Threating Alarm Mining Method for Cloud Security Management,” *IEEE Access*, vol. 6, no. 201706285018, pp. 22634–22644, 2018, doi: 10.1109/ACCESS.2018.2823724.

[10] S. Gupta, S. Jain, and M. Agarwal, “Ensuring Data Security in Databases Using Format Preserving Encryption,” *Proc. 8th Int. Conf. Conflu. 2018 Cloud Comput. Data Sci. Eng. Conflu. 2018*, pp. 214–218, 2021, doi: 10.1109/CONFLUENCE.2018.8442626.

[11] J. Chase, D. Niyato, P. Wang, S. Chaisiri, and R. K. L. Ko, “A Scalable Approach to Joint Cyber Insurance and Security-As-A-Service Provisioning in Cloud Computing,” *IEEE Trans. Dependable Secur. Comput.*, vol. 16, no. 4, pp. 565–579, 2019, doi: 10.1109/TDSC.2017.2703626.

[12] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. H. Ngu, “CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 367–380, Feb. 2020, doi: 10.1109/TPDS.2015.2408613.

[13] S. Kaushik, “Cloud data security with hybrid symmetric encryption,” *IEEE*, pp. 0–4, 2021.

[14] G. A. Prajapati, S. S. Satav, S. Dahiphale, S. More, and P. N. Bogiri, “Cloud Computing Security : From Single to Multi-Clouds using digital signature,” *IEEE Access*, vol. 2, no. 6, pp. 204–213, 2014.