Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 10, October 2021: 5223-5236

A Lattice-Based Certificate Less Management Using M-Tree Hashing Technique for Detection of Malicious TPA

Akheel Mohammad
Assistant Professor
Shadan Women's College,
JNTUH,Hyderabad,Telangana,500085

D Vasumathi
Professor
Department of Computer Science and Engineering,
JNTUH,Hyderabad,Telangana,500085

Abstract: The cloud server is popular for its data storage and security. In traditional approaches, to provide integrity or validity, there exists either identity-based encryption or public-key encryption. Both these techniques are overhead because of certificate management. There is one more serious issue i.e., cloud service providers knowingly or unknowingly may delete the unvisited data. So to remove the data with proper authorization and to control the malicious TPA's, the proposed system implements a lattice-based certificate-less authentication mechanism. It also enhances the search process using multi ciphertext instead of single ciphertext. It also improves the efficiency of the KGC and reduces the space complexity, which is the major constraint for the cloud. The hashing function implemented in this architecture is collision-free and is constructed using a tree data structure popularly known as "Merkle Tree".

Keywords: Lattice, Certificate less, Malicious TPA, Merkle Tree, and Hash-based encryption mechanisms.

Introduction:

In cloud architecture, PKI framework the authentication between the server and users is processed using the digital certificate to prove the integrity of the data uploaded by the user. Many researchers designed various techniques to improve the digital certificate process and to reduce the burden on certification authority. The main advantage of the digital certificate its protects the data from attackers by implementing advanced encryption techniques and the certification authority issues unique certificates for each block separately and each block should be validated by the TPA. Because of this huge amount of data validation, there is every chance for the TPA either to skip the data validation or manipulate the data. So, few researchers started working on the certificate less management to authenticate the data. There exist three types of certificate-less management techniques to encrypt the data provided by the user. The classification of the encryption techniques is illustrated in figure 1.

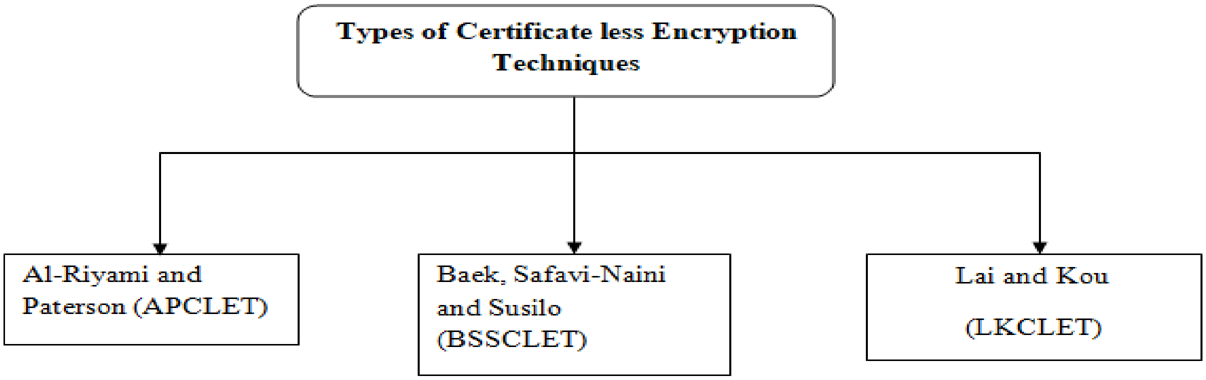
Types of Certificate less Encryption Techniques
Al-Riyami and Paterson (APCLET)
Baek, Safavi-Naini and Susilo (BSSCLET)
Lai and Kou (LKCLET)

Figure 1: Classification of CLE Techniques

In APCLET, the key generation center (KGC) shares the partial key, which is secret from the receiver. In this mechanism, the receiver communicates with the sender using the public key. The main drawback of this mechanism is the public key publishing is possible only till the partial key is generated. In BSSCLET, the sender and receiver simultaneously share the partial and public key but the drawback of this technique is the encryption involves an 8-bit process, which can easily tamper. In LKCLET, the KGC communicates with the receiver bi-directional with the help of necessary protocols but still, the receiver communicates with the sender using a public key only. Once again, the involvement of protocols is a risky and complex process.

In all these techniques, a 5-Step approach is implemented in which the first involves the initialization and setup process of key generation center, it utilizes master public and private key to create a partial key and is combined with SSL certificate and is send to the certification authority for final approval. In the second step, based on the request arrived it matches the user id with the partial key and extracts the necessary information about the user. The third step deals with the key generated using the public key they authenticate the digital certificate but it need not get validated by the TPA, as in the case of the traditional approach. The next two steps involve the encryption and decryption process. The encryption process involves the generation of a cipher text in a block structure format. All these techniques implement the double encryption mechanisms and it also supports recovery mechanisms during any step of the architecture.

Literature Survey:

[1] One of the extensively used assistance in the cloud is its ability in providing storage. Many of such assistances were shared among different other assistance providers with distinguished OS, usually named owned by other groups. The assistance providers manage and work out the various information repository benefits. Here, we concern about the stability of the data that will

be withheld by the outsiders. Even though many communal investigation schemes that overlook TPA were introduced, they were built on standard techniques of cryptographic systems. The goal of this research is to provide a vulnerable and effective certificate less general scrutiny module CL – PAS within the cloud repository. This method can also effectively work on identifying the intruders that forge the investigation method to get access to the TPA to pass validation and forbids curious TPA to get back the true information from the proofs of investigation, thus gaining strength in confidentiality.

[2] With the popularization of cloud utilities, many people opt to use those friendly and affordable assistances thereby saving time, money and gaining security. But for the cloud holder, it will be a concern in managing and securing the service. So, he extends to gain help from outsiders to withhold the customers. In this process, the actual owner of the information cannot hold his authority and it will be transferred to the server cloud and a serious concern instability arises. For this issue, RDIC titled method that helps in providing the rights over a data to its actual owner is developed by gaining the confidence of the customer was proposed. But many of these models uses PKI and identify depended on RDIC does not require repository management. So, a certificate less RDIC was developed to manage confidentiality and rightfulness.

[3] With the abundant usage of technological advancements in various fields, data management operations of numerous customers have been simpler for different assistances like accumulation and analyzing, etc. With this, the growth of the accessibility providers has also increased to meet the requirements of the customers with various liabilities. But most of the users do not know the consequences of using such services that mainly use outsiders to manage the cloud. These disadvantages include stability with the information, the privacy of the data, and rightfulness to the customers by losing the authority over their information. This research proposes two accurate models that work on maintaining the issues of this matter where the customers need not rely on PKI's by introducing CL – PKC as cryptanalysis.

[4] With the rising number of users in the cloud, the provider of the cloud restricts the number of resources to a confined number of customers for simpler management. To maintain and trace the stability in a cloud for scrutinizing information modules, it's better to now the previous step we have taken so that we can get back to the original record when any deceit happens in the transactions. To deal with such difficulties, the researchers in this paper have opted to use the advantage of the blockchain that is indeed applicable in the digital affair of money. This information scrutiny system is a CLS-based methodology that can be applicable invalidating the customers' integrity. To gain robustness, we eliminate key swapping which revokes the users of the system. This causes abolishing customers and verifying the labels and update them in order. A GM of the model rearranges the sign for affirmative customers with the remaining abolished users.

[5] Even though we can be accessible for the assistance of the cloud that provides many divergent resources in different aspects for its customers, it has its limitations mainly for contributing confidentiality for the communication channels in and out of the cloud. One such prominent issue is dealing with the scalability of information. Many innovations have been led for PDP models to manage those issues, but only a few have dug into maintaining the confidentiality problems with the information that needs to be uploaded with stability by the user. The researchers have developed a PDP technique that effectively audits the scalability of data in a mutual workspace while maintaining the confidentiality of the customer. The developed consolidate mechanism of the developed PDP process which is an authorization less cryptosystem eradicates both the key production issue and authentication management issue.

[6] By opting for cost reduction measures over multiple issues with data storage, required resources, etc., and many developers were choosing cloud as a great foundation. But a user could not have complete authority over his data as the cloud is shared among the outsiders for better reliability, there is no proof about the storage of a customer's information and its confidentiality. Most applications use standard measures to overcome these issues instead these have derived many new ones too such as, crypt analyzing public keys, and generating an authentication note. With the modernizing of advanced systems, these could be vulnerable to duplicity. For this, PSCPAC with frame supposition that can eradicate the necessity of the complexity of managing the authorization in PKI – depended on models, abolishing the essential key proposal issue in integrity-based public investigation models, and making the system accustomed across computer attacks.

Proposed Methodology:

In traditional approaches, the certificate management is done by the TPA using the public and private key generations, which increases the overhead latency on the cloud which in turn impacts the load balancing factors in an adverse direction. So, the proposed system implements a hybrid lightweight certificate-less authentication process, which involves the usage of Lattice-based Merkle Hash Tree (LBMHT). Merkle Tree is a data structure, which helps in the process of authentication by using hash functions. Every root and internal node in the tree represents a block of data and the leaf node contains the data of the block in an encrypted format. The main advantage of this algorithm is, every leaf node generates a unique ciphertext for different blocks of data. This is a bottom-up recursive approach, which is continuous until a single block of hash code is generated. The main advantage lies in its linear search time because the searching process involves only important hash codes retrieval, it is doesn't work on the block by block retrieval process. In the proposed algorithm, it defines a simple relation between key and value to generate new blocks based on the pairs, it is utilized.

Pseudocode for generating Hash Values for the blocks:

```
Input: Data Block, D
Output: Encoded Data Block, ED
Begin
1. Initialize an UTF coded integer
2. if(len(D)==0) return 0 else lh←len(D)
3. h(K,V)← D mod tree_size
4. acc←acc||len(h(K-1,V-1))
5. for i←acc to 0:
   a. encode_data[i]←children(h(K[i-1],V[i-1]),acc)
End
```

The main advantage of the certificate less cloud server is, KGC component does need not maintain the private keys of the different users and the public keys certification burden is reduced on the certification authority. During this certificate less model construction, there is the possibility to get errors. So, the system needs a mechanism, which can automatically learn its mistakes from the errors it has generated. The best component for this type of implementation is "Lattice". It is represented a group of independent vectors on which sampling algorithms can be applied. The major goal of this problem is to define an objective function that finds the decision parameter and its corresponding value by analyzing the error parameters. To overcome drawbacks of the existing CLET, the proposed algorithm uses 6-tuple representation instead of 5-tuple representation. This is illustrated in figure 2.

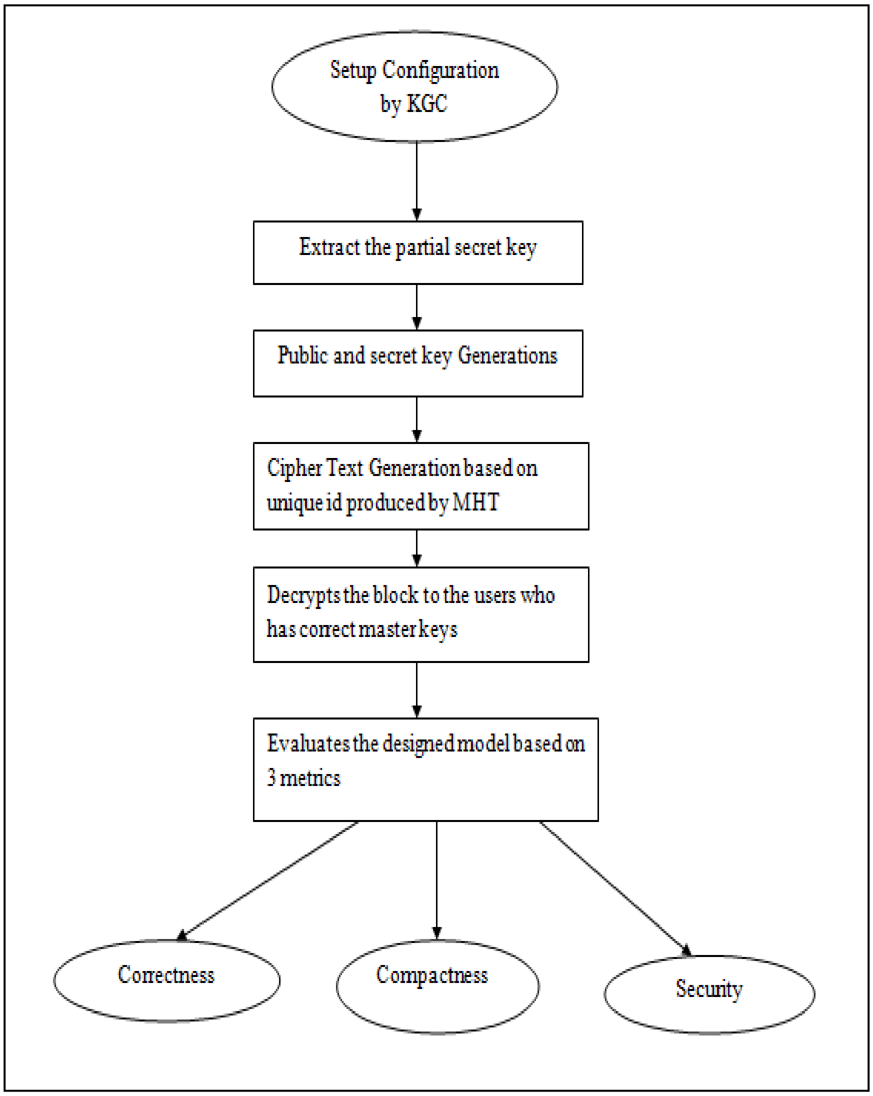
Setup Configuration by KGC
Extract the partial secret key
Public and secret key Generations
Cipher Text Generation based on unique id produced by MHT
Decrypts the block to the users who has correct master keys
Evaluates the designed model based on 3 metrics
Correctness
Compactness
Security

Figure 2: Integrity Process to Data of users

1. Initial Setup: This phase is configured by the KGC component by setting the random parameters for the security entities as defined in (1)

$$\mathrm{sec}[i] = \alpha * Latt[i] \ \text{ - (1)}$$

Now define the security matrix which contains gradient functions and also define an objective function with the inverse operation to transform the given matrix into tensor notation. A random matrix is generated by using a genetic-based approach and set the hash code to MHT value. So, the initial setups produce master public and secret keys for further communication with the other components.

2. Extraction of partial secret key: Initially compute unique id for every entity by using (2)

$$unique\_id[i] = \ MHT(\mathrm{sec}[i])\text{- (2)}$$

This stage mainly performs two sub-tasks; one is the generation of digital signature for the entire block by using the famous SamplePrep() algorithm and the second is the verification process to authorize the encryption process.

3. Key Generation: By using the above generated partial secret key, public keys are generated using (3)

$$\begin{pmatrix} X_i \\ X_j \\ X_k \end{pmatrix} = \begin{pmatrix} uid_i \\ uid_j \\ uid_k \end{pmatrix} \text{- (3)}$$

The following steps compute the remaining steps after transforming into the above tensor.

a. Assume M= M.$\begin{pmatrix} X_i \\ X_j \\ X_k \end{pmatrix}$mod z

b. Assume U= U. $\begin{pmatrix} unique\_id_i \\ unique\_id_j \\ unique\_id_k \end{pmatrix}$ mod z

c. Output= $\begin{pmatrix} -X \\ -U \\ -1 \end{pmatrix}$

4. Cipher Text Generation: The encrypted data is produced by creating 3 random matrices, which are operated through noisy Eigenvectors. The decryption process involves matrices multiplication and the addition of ciphertexts generated.

Results and Discussion:

The proposed system is compared with certificate-based systems and results are represented in table 1.

Table 1: Comparative Study on Time

Size in MB	Time with Certificate	Time Without Certificate
25	210989	200170
50	235610	211674
75	243672	221093
100	256249	233092

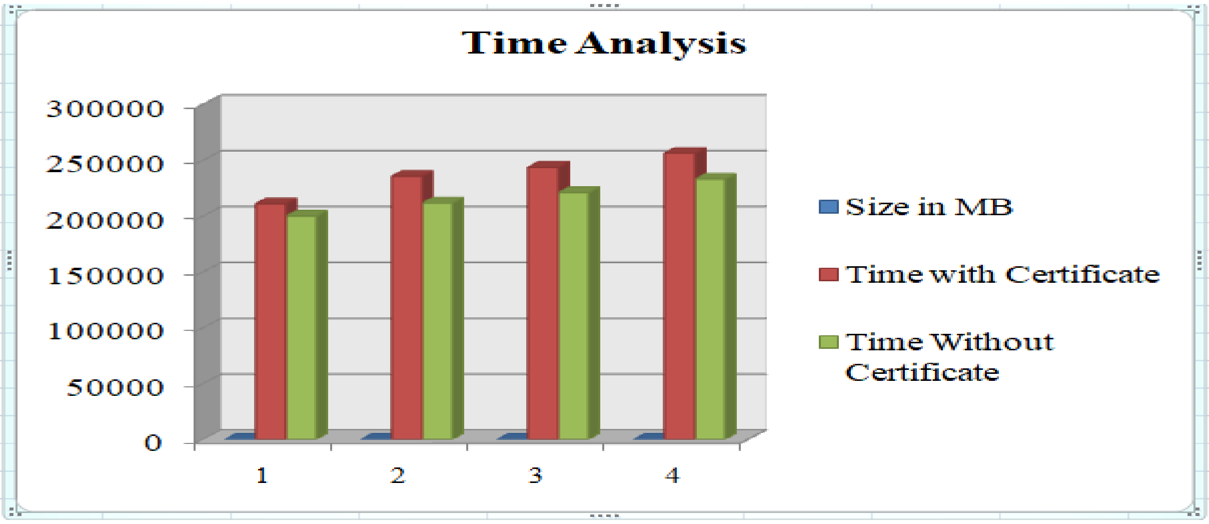

Figure 3: Time Analysis on Certificate versus Non-Certificate

Figure 3, states that without the certificate mechanism only it has achieved less time and in the figure, the x-axis represents the size in MB and the y-axis represents a time to execute the necessary operations like integrity, encryption, and verification.

Now let us see the comparative study on the certificate fewer systems proposed in the introduction based on the accuracies, response time, and execution times obtained, which are represented in table 2.

Table 2: Existing CLET, Previous Developed versus Proposed Performance

Algorithm/Metric	Accuracy	Execution Time	Response Time
APCLET	87.81	309817	100233
BSSCLET	80.22	357721	129034
LKCLET	86.59	305174	108931
CUCKOO+AES	88.45	294189	99254
Retrieval	89.29	265593	96408
Proposed	90.37	233092	95525

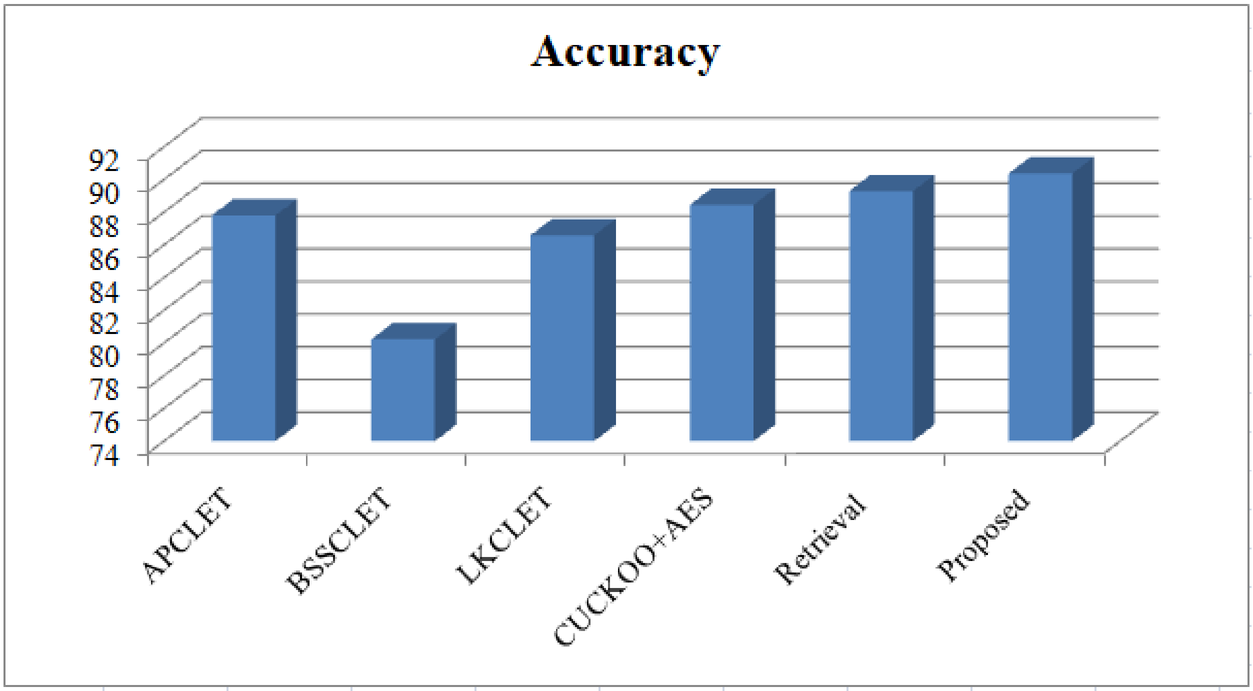

Figure 4: Efficiency of Proposed System

Figure 4 states that the proposed system has good accuracy and the system has performed a comparative study on 100 MB File size. The X-axis represents different certificate-less mechanisms and Y-axis represents the accuracy of the model.

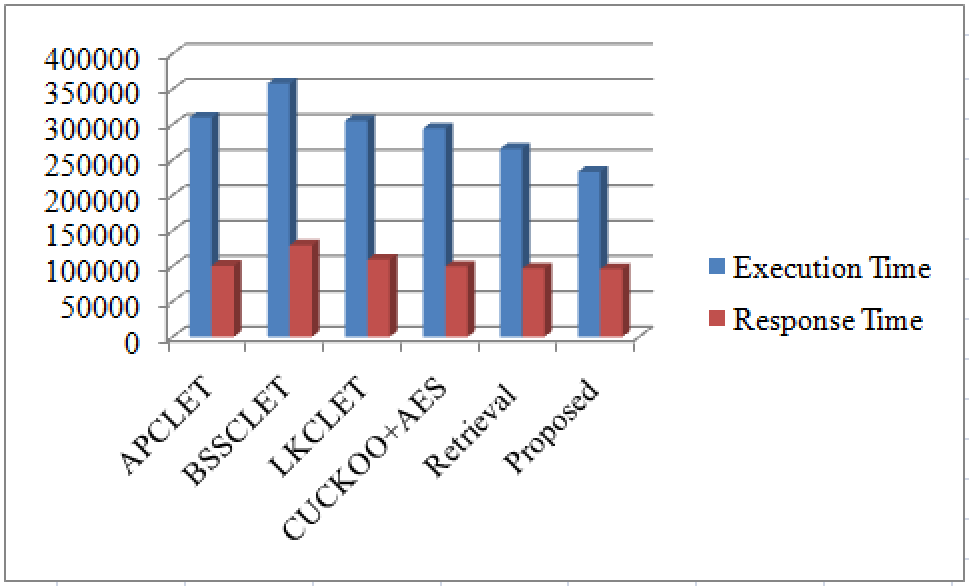

Figure 5: Execution and Response Time of Certificate less technique and Proposed Techniques

Figure 5 denotes that the proposed system has less execution time and response time when compared to other CLE techniques. The X-axis denotes techniques and Y-axis represents a time to execute and respond for 100 MB block size in a file.

Table 3 compares the encryption time of different algorithms, and it also states that the proposed algorithm, which uses a tree data structure, further reduces the encryption because of the hashing technique involved in it

Table 3: Time to Encrypt the file blocks

Input Size in MB	**RSA**	**AES**	**Cuckoo+AES**	**Retrieval Algorithm**	**Proposed Algorithm**
100	0.635	0.61	0.584	0.57	0.52
150	0.685	0.643	0.602	0.6	0.591
200	0.713	0.699	0.681	0.633	0.64
250	0.775	0.742	0.71	0.70	0.696
300	0.895	0.878	0.85	0.79	0.743

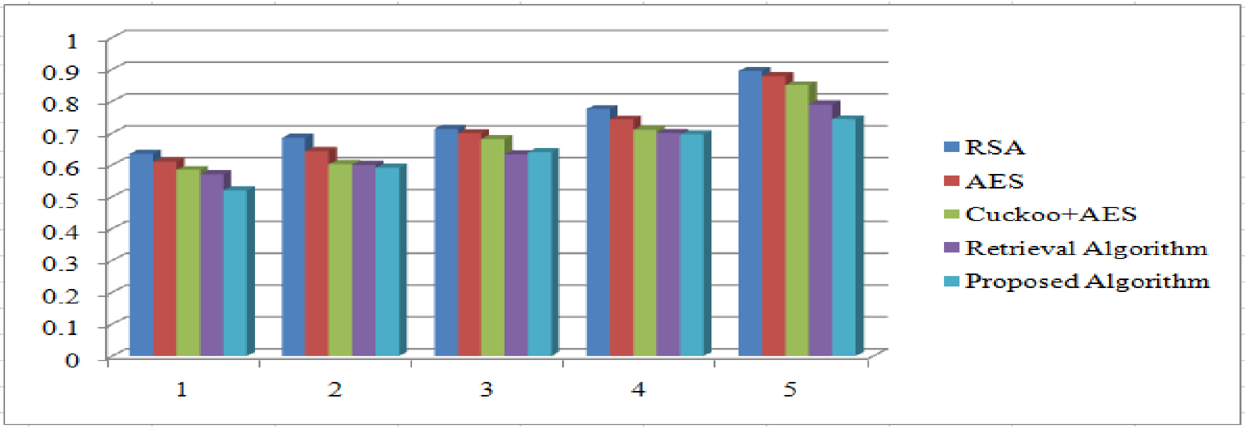

Figure 6: Encryption Time Analysis

In Figure 6, proposed algorithm takes much less time than the Genetic and security algorithm combination. On X-axis, it denotes the size of file in MB and on Y-axis, it denotes the time to encrypt the data blocks .Table 4 projects the efficiency in terms of decryption time by comparing with the previous models that exists in nature.

Table 4: Time to decrypt the file blocks

Input Size in MB	**RSA**	**AES**	**Cuckoo+AES**	**Retrieval Algorithm**	**Proposed Algorithm**
100	0.815	0.793	0.629	0.61	0.591
150	0.887	0.809	0.653	0.64	0.62
200	0.891	0.823	0.701	0.694	0.678

250	0.902	0.874	0.724	0.722	0.721
300	0.912	0.883	0.744	0.74	0.73

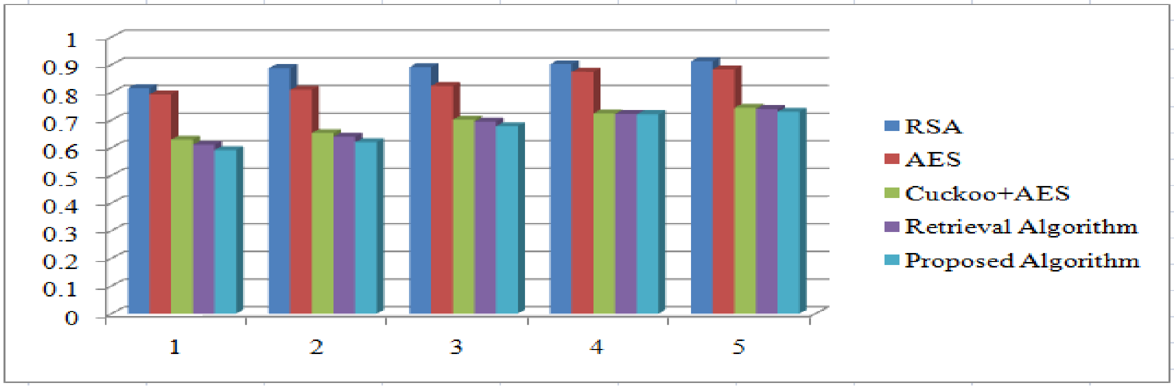

Figure 7: Decryption Time Analysis on data blocks

From figure 7, the proposed algorithm also takes less time to decrypt the file than the other algorithms. Similar to the figure 6, X-axis represents block size in MB and Y-axis represents the time to decrypt the files. Table 5 represents the utilization of memory and is compared with other algorithms

Table 5: Memory Utilization Analysis

S.No	**Algorithm**	**Memory Utilization in MB**
1	RSA	160
2	AES	135
3	CUCKOO+AES	108
4	Proposed Algorithm	96

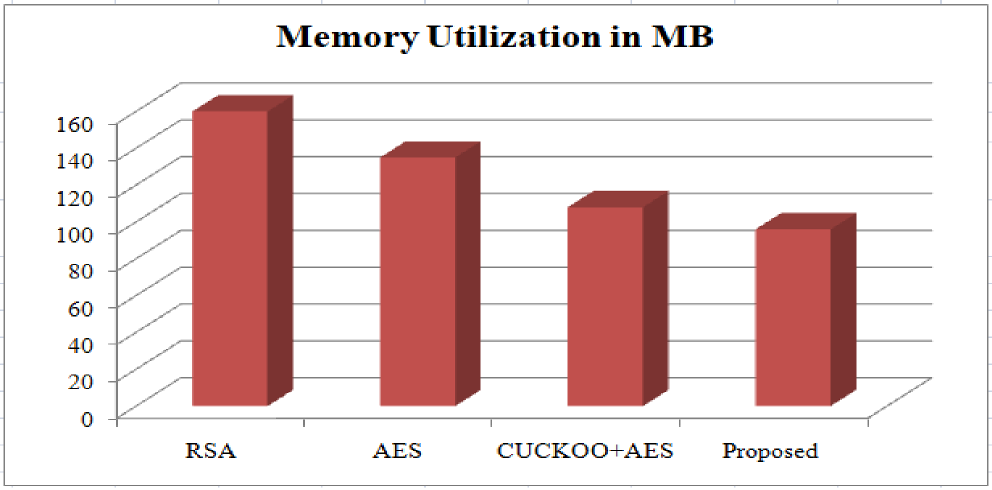

Figure 8: Memory Utilization by Different Algorithms

In Figure 8, X-axis represents the previous algorithms RSA, AES and CUCKOO AES, the proposed algorithm and Y-axis represents the amount of memory utilized in MB, to execute a data block.

All the below results are executed using the Cloud Sim tool, The cloud developers were allowed to verify and validate the policies they maintain in an advancing and a sustainable environment for free. It is much advantageous in tuning the impediment before practical deployment. Moreover, this tool does not require any proper software to deploy as it is a simulator. This tool is more detailed and protected in designing and experimentation. It is also friendly in updating the user requirements without any trouble or using a high-end computer.

Table 5: Execution Environment Parameters

Conditions	**Statistics with traditional approaches**	**Statistics with CUCKOO+AES**	**Statistics with Replica Algorithm**	**Statistics with Proposed Algorithm**
Number of Chassis Switches in L4	1980	1980	1980	1980
Packet Size	1260 KB	1000KB	908 KB	823 KB
Line cards at L4	1630	1630	1630	1630
Ports at L4	72	72	72	72
Number of racks at L4	16	16	16	16
Number of Chassis Switches at L3	432	432	432	432
Line Cards at L3	164	164	164	164
Ports at L3	48	48	48	48
Number of racks at L3	128	128	128	128
Used virtual machines	1800	1361	1249	1043
Number of Servers	64	58	56	52
Maximum number of Cloud Service Users	18000	15642	14318	13651
Hosts in each rack	132	121	113	107
Each Host supports	16 processors	4 processors	4 processors	3 processors
Memory with each processor	256 GB	64 GB	64 GB	64 GB
Storage Memory	512 GB	128 GB	128 GB	64 GB
Virtual Disk Memory	430 GB	430 GB	430 GB	430 GB
Bandwidth for L4	256 GB/Sec	128 GB/Sec	128 GB/Sec	128 GB/Sec
Bandwidth for L3	128 GB/Sec	56 GB/Sec	56 GB/Sec	56 GB/Sec
Bandwidth for L2	64 GB/Sec	32 GB/Sec	32 GB/Sec	32 GB/Sec
Bandwidth for L1	16 GB/Sec	8 GB/Sec	8 GB/Sec	8 GB/Sec
Queue delay	0.005 Seconds	0.000 seconds	0.000 seconds	0.000 seconds
Burst time	0.0056	0.0018 seconds	0.0010	0.0007 seconds

	Seconds		seconds	
Idle time	0.0032 Seconds	0.00005 seconds	0.00005 seconds	0.00003 seconds

Table 6 now compares the final parameters regarding the TPA, to identify the malicious attackers to improve their truthiness' values to work regarding the communication block costs

Table 6: TPA Parameters Analysis

S.No	Methodology	Communication Cost	Number of Malicious Attackers	Dishonest Rate	Storage Required
1	PPP	900	2	5%	800 KB
2	CUCKOO+AES	883	2	4%	750 KB
3	Retrieval	714	1	3.75%	698 KB
4	Proposed	649	1	3%	550 KB

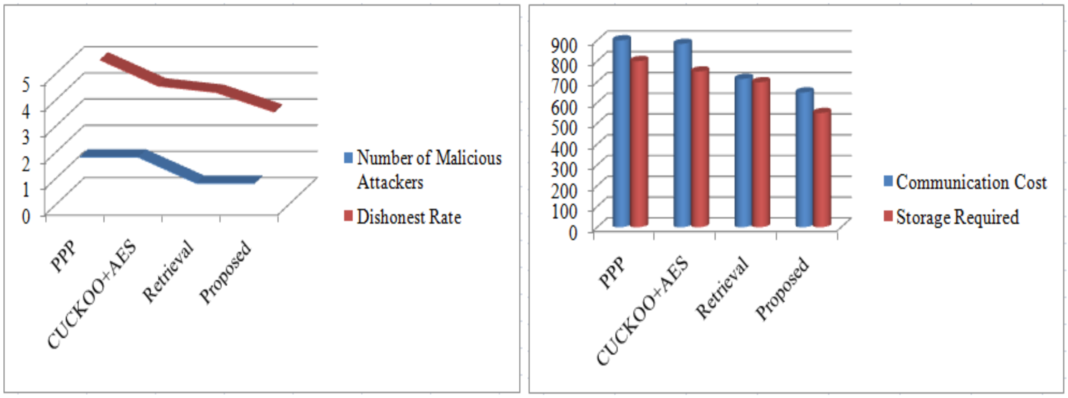

Figure 9(a) & 9(b): Different Parameter Values

From Figure 9, the dishonest rates and storage rates are reduced. It also observed that number of malicious attackers is also reduced. It is showing improvement towards removing the malicious Auditors.

Conclusion:

The main advantage of this M-Tree data structure is it helps in dynamic operations performance in a linear amount of time. Using the lattice matrix representation reduction of energy consumption the server nodes take place and the cloud service provider manages the resources in the distributed environment very effectively. TPA need not verify every digital signature of the block; it has to take care of a single authentication code generated at the end. The proposed system aims to preserve privacy and tries to execute the operation with a minimum number of resources. The simulated results have proved that the proposed model is efficient in terms of accuracy, time complexities, and other parameters also.

References:

[1] Gao, G., Fei, H., & Qin, Z. (2020). An efficient certificateless public auditing scheme in cloud storage. Concurrency and Computation: Practice and Experience, 32(24). https://doi.org/10.1002/cpe.5924.

[2] R. Zhou, M. He and Z. Chen, "Certificateless Public Auditing Scheme with Data Privacy Preserving for Cloud Storage," 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA), 2021, pp. 675-682, doi: 10.1109/ICCCBDA51879.2021.9442586.

[3] Zhang, J., Li, Z., Wang, B., Wang, X. A., &Ogiela, U. (2020). Enhanced Certificateless Auditing Protocols for Cloud Data Management and Transformative Computation.Information Processing & Management, 57(6), 102287.https://doi.org/10.1016/j.ipm.2020.102287.

[4] ZHANG, Yinghui; ZHANG, Tiantian; XU, Shengmin; XU, Guowen; and ZHENG, Dong. Revocable and certificateless public auditing for cloud storage.(2020). Science China Information Sciences. 63, (10), 1-3. Research Collection School Of Computing and Information Systems.

[5] Yan, H., Liu, Y., Zhang, Z., & Wang, Q. (2021). Efficient Privacy-Preserving Certificateless Public Auditing of Data in Cloud Storage. Security and Communication Networks, 2021, 1–11. https://doi.org/10.1155/2021/6639634.

[6] Li, H., Wang, Y., Fu, X., Lan, C., Wang, C., Li, F., &Guo, H. (2021). PSCPAC: Post-quantum secure certificateless public auditing scheme in cloud storage. Journal of Information Security and Applications, 61, 102927.https://doi.org/10.1016/j.jisa.2021.102927.