A Four-Layer Robust Storage in Cloud using Privacy Preserving Technique with Reliable Computational Intelligence in Fog-Edge

E. Nirmala[1*] and S. Muthurajkumar[2]
[1&2]Department of Computer Technology, Madras Institute of Technology Campus,
Anna University, Chennai-600 044, India
[e-mail: nirmalalochan@gmail.com ; muthurajkumarss@gmail.com]
*Corresponding author: E. Nirmala

Received March 9, 2020; revised May 26, 2020; accepted July 27, 2020; published September 30, 2020

Abstract

The proposed framework of Four Layer Robust Storage in Cloud (FLRSC) architecture involves host server, local host and edge devices in addition to Virtual Machine Monitoring (VMM). The goal is to protect the privacy of stored data at edge devices. The computational intelligence (CI) part of our algorithm distributes blocks of data to three different layers by partially encoded and forwarded for decoding to the next layer using hash and greed Solomon algorithms. VMM monitoring uses snapshot algorithm to detect intrusion. The proposed system is compared with Tiang Wang method to validate efficiency of data transfer with security. Hence, security is proven against the indexed efficiency. It is an important study to integrate communication between local host software and nearer edge devices through different channels by verifying snapshot using lamport mechanism to ensure integrity and security at software level thereby reducing the latency. It also provides thorough knowledge and understanding about data communication at software level with VMM. The performance evaluation and feasibility study of security in FLRSC against three-layered approach is proven over 2^{32} blocks of data with 98% accuracy. Practical implications and contributions to the growing knowledge base are highlighted along with directions for further research.

Keywords: Fog Computing, Edge Computing, Malicious Attacks, distributed computing, Solomon code algorithm, VM-Monitoring and Computing Intelligence.

http://doi.org/10.3837/tiis.2020.09.017 **ISSN : 1976-7277**

1. Introduction

The strategically developing cloud computing technology has an impact on storage. Due to the enormous volume of data generation out of social media like Twitter, in which around 500 million account holders tweet per day and 60 hours of video uploaded per minute on YouTube. Aclassic example is the Facebook 50 million accounts holders content-leakage that surfaced in September 2018. Such problems emerged due to paucity in bandwidth, inefficient network interconnections inherent in Virtual Private Network (VPN) and in the case of private cloud and Storage Access Network (SAN) through Network Interface Card (NIC). Data security issues came about due to distributed cloud server where the migration takes place inevitably in business environment. Wireless network developers are not wholly ceased with the efficacy and potency of Computational Intelligence (CI) algorithms. On the contrary, Computational Intelligence researchers are not acquainted with the complete nuances and bottlenecks faced in wireless networks. The present paper bridges this dichotomy with respect to distributed storage data for enhanced integrity and prevention of malicious intrusions.

1.1 Scope and Objective

The focus of the present paper is to resolve the latent security gap in cloud computing by using Virtual Machine Monitoring (VMM) technique as an additional layer to the prevailing three layered configuration.

The primary objective is to provide multi-level, decentralized cloud storage in an open and secure environment.

1. To preserve integrity of data while migrating to and from the cloud servers.
2. Preserve data security, Privacy Protection and Intrusion Avoidance for improving storage efficiency of cloud servers.

The scope is delimited to software and firmware which prevents broaching upon any kind of communication system per se. However, any description on wireless communication or antennae is with a view to enhance clarity.

Hence in this work secured transmission is achieved with the existing Tiang Wang's (TLS) approach with timestamp kind of monitoring by setting global time before data gets transmitted through the communication channels.

Though it is sosftware based security, Galois discipline related implementations are used to increase the robustness in security which exists in storage devices. Moreover system detects the intruder through Galois check with VMM that increases the reliability. The efficiency of reliable communication can be measured in terms of encoding/decoding technique by applying valuable parameters against number of data blocks, size of blocks, kind of stored data (audio, video and text). Thus the storage efficiency is validated against index efficiency.

Even though the edge devices are closer to the user machine, the intelligence part exists in providing secured transfer with reduced delay time [1]. Resilience servers can access small part of data to reduce the work load of CSP. Hence cloud edge servers reduces the cost of transmission [2]. Such extended technology gets implemented to reduce the delay time in bus services by using deep learning technique [3].

The plethora of IoT's and ever increasing outreach of the internet has spawned exponential growth in mobile traffic. To address this spiralling demand for data handling in addition to inadequacies existing in digital networks, devices will have to be reconfigured for MIMO systems. Communications with high data rates of transmission employ meta-material (MTM) beam-steering antennae [4], [5]. The 5G wireless communication operating over larger frequency bandwidth using ultra-wideband (UWB) synthesized antennas offers one such THz-Band applications solution [6].

Use of a monopole radiator with concentric split-ring resonators enable fractional bandwidth of the antenna enhancement from 41 to 87% [7]. There are other compact, miniature and microstrip multiband antennas for smooth switching between networks [8],[9] that lends easily in bracing the speed, latency, and above all cost-effectiveness based on composite right/left handed transmission line (CRLHTL) metamaterials. It enables long range access at low cost, thereby making it excellent application for distribution and logistics systems besides small footprint, global portability and excellent radiation characteristics [10], [11].

1.2 Four-Layer Robust Storage in Cloud (FLRSC)

Section 2 provides a brief overview of related work prior to FLRSC architecture, and its pros and cons. Section 3 brings out a comprehensive outline of Four Layered Privacy Preserving (FLPP), its process, mechanism and integrity of stored data with its relationship in communication network. Section 4 presents algorithm for distributed data storage approaches in addressing the several issues that arise in data security in cloud environment. Next, the practical implications are outlined in Section 7.

Finally, conclusions and authors' suggestion on future directions of applying FLRSC and CI methods to various data security and privacy problems are laid out in Section 6 followed by conclusion in Section 7.

2. Related Work

Due to the evolution of Internet of things (IoT's) an automatic diversion of storage technology in terms of smart edge devices has been introduced. Such edge storage device helps any user to take harmless decision concerning stored data, and hence forwards the same in a smarter way to shared pool of resources.

The authors having carried out an in-depth review of existing literature and on examining the empirical studies have suggested a method of overcoming this gap in data security, particularly in the context of cloud computing and its allied forms in data storage. The gap analyzed reveals an emerging need of synchronized cloud computing with Fog Computing by means of Intelligence systems and found the advantage in providing emphasis to storage management systems associated with IoT, where the edge devices like smart phones, desktops, and healthcare wearable devices are connected through Integrated Access Devices (IAD's) irrespective of the type of network [12].

Pervasive computing system nearer to network is introduced to fix the limit of an application running onto the distributed server. There is a requirement to provide efficiency and security at reduced cost [13]. The approach envisaged in overcoming the problem is by using layered algorithm implementation with machine learning technique.

2.1 Privacy-Preserving Fog and Edge Computing System Model

Cloud paradigm works with IoT's connected with huge number of devices in real time. Edge-computing ensures better control over traffic, in network flow. More attention rendered to group nodes and check for the availability of data during transmission. This is achieved by applying double trap-door crypto system, thereby achieving low latency and increased bandwidth [14].

Abubaker et al. [15] discusses about two different approaches upon the closeness of fog nodes to the users with the interconnected application while aggregating the nearer nodes for ensuring the security by using the Trusted Third Party Node Scheme (TTPS). The advantage of this TTPS scheme is reduced latency and overhead costs. At the same time CI brings about survivability due to flexibility, and robustness against dynamic topology variations, and infallible communication.

2.2 Detecting Unstable Sensors and Augmenting Security

In future IoTs oriented devices and liberal use of the Sensors would take place for detection and prevention of faulty data. Fog assisted sensors are used in quick decision-making and load balancing. The implementation is carried out with intelligence algorithm to distributed network of Hungarian methodology [16]. The advantage of using such system results in increasing the Quality of Service (QoS) by reducing the relay time in load balancing.

2.3 Optimized Task Scheduling Algorithm for Image Assignment

The primary goal of above said setup is to entrench the conventional system and strengthening the fog-computing environment with high security, achieved by using job imagery descriptions laid in the storage servers [17]. It is noteworthy to propose a well-organized job development and source organization process within a minimum span of time via min-max non-linear programming.

Energy consumption is high in conventional system. To overcome this problem, communication between fog to cloud and cloud to distributed node, a novel system is developed with wireless sensors. In this way time is reduced due to minimum packets transmission gaining an advantage of 97% accuracy and time span limited for transmission upto 180 nano seconds [18]. Research in traffic classification, which avoids payload inspection, has accelerated over past five years. It is generally difficult to compare different approaches, because they vary in the selection of features (some requiring inspection of packet payload), choice of supervised or unsupervised classification algorithms, and set of classified traffic classes.

2.4 Position based Networking Facility

Position Based Networking works at the edge of the networking for achieving efficiency and reduced latency and to increase the confidentiality of the users. It could be achieved by using machine learning techniques for the mobile users. The Real-time information about industries is processed using the service providing stations [19]. Later, in the early 2020's the confidentiality to the industrial informatics would evolve by using green model with cyber physical model thereby reducing the communication cost with less energy [20].

During transmission, the nearer nodes in the network consumes more energy that sometimes may lead to nodal death. Such failure in the routing path can be resolved by

providing optimal monitoring to sensor nodes, using BAT algorithm which increases the catastrophe survivability of the nodes [21].

Even though resource allocation (RA) to suitable demanding node is optimized, allocation is expected to reduce the cost of communication. Whale Optimization Algorithm is used in IoT's to optimize the service by reducing time and energy is an added advantage [22].

A wide range of earlier approaches can be seen in the comprehensive survey conducted by Nguyen and Armitage (2020) where an Optical Tunnel Network System was proposed, in which the electrical switching circuits were replaced with optical switching system besides adding Artificial Intelligence (AI) thereby reduced the latency and 82.6%. power savings irrespective of the traffic prevailing in the market and load [23]. In addition, it also provides flexibility, scalability and reliability. The advantage of this system due to the reusable characteristic of wavelength helps to achieve high bandwidth during reallocation of tunnels.

In any of the complex networking structure, built with heterogeneous nodes, the algorithm works well with enhanced security through linux type of containers with software protection guard of Intel Processor [24]. By incorporating security model through Docker and Open SGX, a reliable and flexible edge computing in distributed nodes can be achieved. Though the system faces a challenging factor i.e., third party malevolent access.

In the 5G era, couple of problems arising out of network traffic and load balancing are addressed by the L. Zhou et al. [25]. The author used the technique of connecting vehicles in the distributed environment through traditional cloud assisted system, thus enabling interaction with enormous nodes. This innovative construction is location independent. The advantage accrued is reduced latency and high security.

2.5 Wearable Healthcare Devices

In the medical imaging system, accessing time is reduced by using cloud nearer edge system [26]. The system design allows the user to access the medical images within their scope. The problem lies in malicious access which is resolved using fog based protection model designed to safeguard the images. The ultimate beneficiaries are cloud based bioinformatics providers due to implementation of fine grained data access controlling mechanism, to reduce the accessing time with greater accuracy.

In order to enhance security against data storage, a new three-layered protection is introduced against the data present in different layers. To achieve this Solomon hashing algorithm is used along with manmade machine intelligence (AI) [27]. It is achieved through regular monitoring. The advantage of using this system is privacy protection on different layers.

Another area where a secured system with effective security measure has been developed is in user biometrics i.e., facial images. While sharing metadata generated from images either from edge devices or through (IoT) high security is needed. So, author has introduced zero water marking and visual cryptography techniques [28]. Author also resolves security issues, through fog at nearer node in distributed network. The above stated schemes, don't have any adverse effect on retrieving the image data resident either at source or host domain. The resulting advantage is high rate of recognition.

T.Wang has planned for the provision of security to the user data irrespective of their location. Especially in case of mobile users, their personal information may be traced by computing the distribution proportion lodged in cloud, fog, or local machine,at any point of time in the network [29]. The conventional method is called location based system (LBS). In

this paper, the author presents various measures to be taken to provide high security from the application layer that are interlinked with the mobile devices, with the help of location sensors.

3. Four Layered Privacy Preserving

3.1 Four Layer Architecture

Our Proposed system design comprises of four different layers to mitigate the risk of uncertainty in data storage. Aim of this construction is to provide security and integrity to the stored data by following the procedures as depicted in **Fig. 1**. Whenever the data is accessed for processing, immediately, algorithm for the stored procedure disperse the data at various intervals. In this system data dispersion rate is 95%, 4% and 1% in Servers like cloud, fog and local host. Specifically attack gets nullified. To provide security instead of conventional key and encryption standards, for the first time the fourth layer is introduced as VM, to keep track of data dispersion rate along with its functionality.

At first the data block is divided in to (k) number of blocks. Later the block is dispersed into four layers using Hash Solomon algorithm and stored in cloud server (first layer), fog servicing machine (second layer) and in local machine (third layer). Whoever is having the identity key alone can get back the whole data dispersed at three different locations using Reed Solomon Algorithm.

Otherwise partial data alone can be received by the intruder. In addition to the above mentioned three layers there is a fourth layer as VMM. It is used to keep track of the encoding and decoding at equal interval of a time using snapshot technique through lamport algorithm, depicted in **Fig. 1**. This is the novilty introduced by the author in the present work.
Here the work comprises of four layers starting with:

1. Transport Layer: Security Preventing malicious intruder from accessing private sensitive information through dispersion rate control.
2. Archival level security: Storage at the edge devices and Host Cloud Distributed.
3. Network Layer: Fog is closely related with cloud computing in providing security to IoT's.
4. Hypervisor Layer: Software defined Virtual Machine provides security for physical data storage and retrieval.

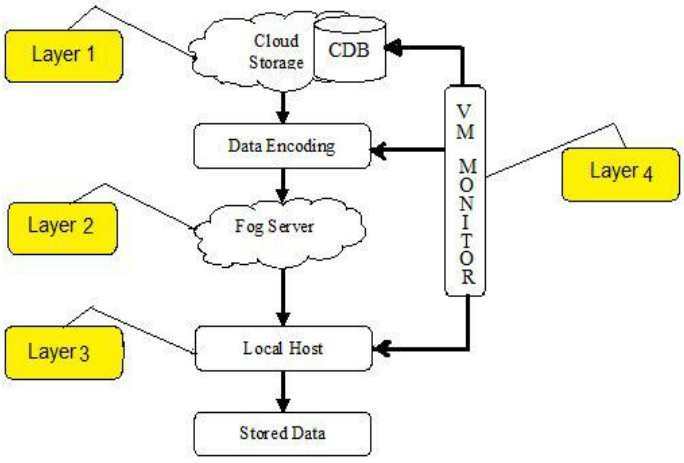

Fig. 1. Proposed four layer approach

3.2 Stored Procedure

Stored procedure blocks are dispersed into three different locations as 95%, 4% and 1% in cloud server, fog server and local host as stated earlier. This dispersion towards stored data will save the data from the third party attack. Even though the attacker tries to attack, he may not find the whole set of data because of the very nature of partial dispersion. The Fourth layer is used to hold the location and size of data stored in different layers in a consecutive manner, which brings in uniqueness to the proposed method of ensuring security in cloud environment.

3.3 Encoding and Decoding

Dispersed data at differentiated layers are encoded using the hash Solomon coding algorithm. Whenever user request for the data is initiated/ received, soon after the decoding process starts receiving 95% of data from the cloud server, by combining 4% of data from the fog server, adding 1% of data with cloud local host, the original user data can be retrieved, by checking with the Virtual Monitoring Layer; where the address of the dispersed data record is maintained in the form of snap shots, in the network path at equal interval of time

3.4 VM Monitor Layer

The user request is preprocessed by validating with the dispersed ratio of data stored in the cloud, and by tracking their location address. Only when encoded data is in sync with the rate, then only it allows the user to download or decode the data. This personalized authentication towards the stored data will prevent intrusion and avoid unauthorized access by the third party in the network, thereby integrity of data is maintained.

4. Algorithms for Four Layered Approach

4.1 Algorithm for Stored Procedure

The building process for four-layer privacy protection helps to store the details of data into a number of blocks. The security to the data file is embedded with an encoding technique. Immediate acknowledgement gets generated for the encoded data by the system in the form of feedback information. In **Fig. 2** based on the assumption that 1% of the data block is stored in the local server remaining data will be stored into the fog server. Finally, the user data is to be sent to the fog server. Then again, by the repetitive encoding using Hash Solomon, cloud server receives the blocks of data and from the fog server as depicted in the diagram. The storage process gets divided into four layer working model e.g., local layer, fog layer, transport layer and cloud layer.

4.2 Algorithm for Encoding

Step1: User exercises the option *select* the file from the list of files available in the cloud storage. As soon as the selection of a file get over immediately encoding of the file starts with hash Solomon Code Algorithm commences.

Step2: After performing the encryption of data, only 1% of the encrypted data is stored in to the local edge device while remaining 99% of the data is sent to the fog server.

Step3: Again encoding the 4% of the data and sends it to the fog server, then the fog server receives the data the fog owner redistributes the data into no of blocks to the storage.

Step4: Finally, the archival/storage ends with different server levels. The algorithm for down loading the file from the cloud server has four steps are as described in the following section.

4.3 Procedure for Decoding

Step1: Based on the user request the cloud server combines a different node server which has been distributed.

Step 2: After the integration, the server in the fog layer receives the user data from the Cloud Server.

Step 3: Encoding is carried out with the 4% data blocks of fog server.

Step 4: By calling step 3, we can arrive at the encoded data and recollect the 99% data, which can be retrieved by the user.

Step 5: Repeat step 1 and 4 to get the complete set of data from three levels of layers in a highly secured manner.

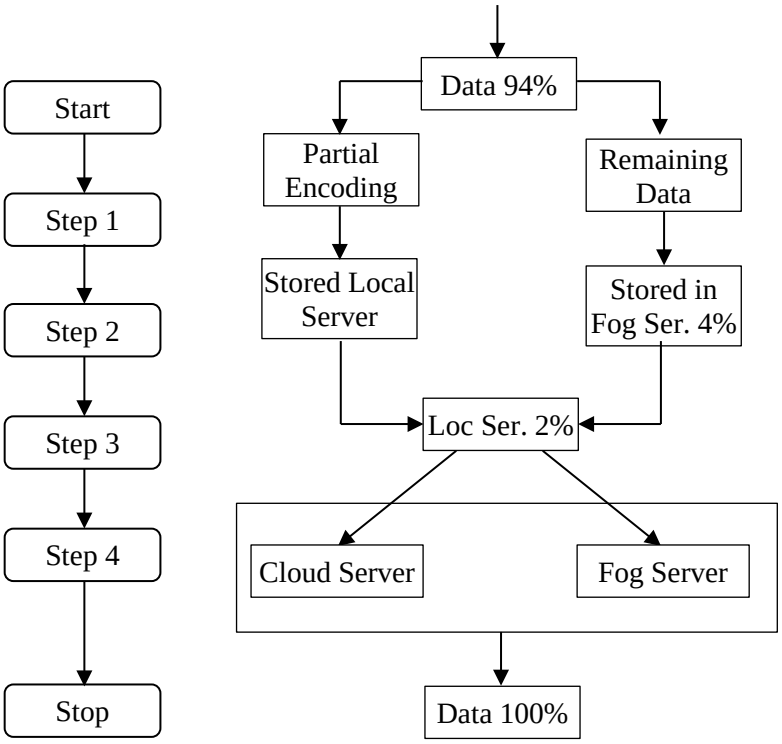

Fig. 2. Encoding Architecture Diagram

4.4 Procedure for Monitoring

The detailed procedure for monitoring/auditing for the validity and integrity of data is based on the security and safety of user sensitive data as well as that of the system provider.

Attested secure enclave that safeguards private sensitive data is accessed by only authorized software thus isolates from a compromised system software of privileged user.

Step1: Based on user request initiation location of the data is identified.

Step2: Check/verify the location id is matching with the dispersion ratio.

Step3: If YES combine the data dispersed at various servers and local host

Step4: Else

Step5: Check the snapshots captured at regular interval of time at network

Step6: End if

Step7: End user request

5. Performance Analysis

The algorithm is executed by segmenting the data file into no of data blocks. Immediately the system used to send the response concurrently, after encoding. Reed Solomon Hash Algorithm is used to process the encoding of data blocks. Based on the assumption, say that 1% block of data, after encoding is to be saved into the local machine. The fog server is loaded with the left over content of 99% of data blocks. Then, Reed Hash Solomon code will be applied while encoding the data stored into local machine. The encoded blocks of data can be encoded once again based on the assumption that 4% of the encoded block has to be moved in to the fog server. Remaining 96% will be stored into cloud server. Finally, the data is received from fog. Whenever all the blocks are stored into the respective server, then the stored procedure meets its end.

The performance of this algorithm described in **Table 1** is comparatively better than the existing system architecture with the stored procedure in the end, we used to save(y_{i1} to $y_{i4)}$ to the cloud server, and we use to save ($y_{i5)}$ and S in the Fog Server where (ket=5,mb=1) and ($y_{i)}$ the encoded matrix. After encoding value is entered in the form of matrix with the identity matrix and Candermone matrix of a Cauchy matrix. At last, we store Y_1 to Y_4 in the cloud server and store Y_5 and R in the fog server (k = 5, m = 1).

Table 1. Galois Cracking with a quantity blocks

Galois Field	N	V	Time of Exhaustion
X1=nF(24)	1	6	256^3
X2=nF(24)	1	6	256^3
X3=nF(20)	1	6	256^3
X4=nF(20)	1	6	256^3
X5=nF(21)	1	6	256^3
X6=nF(216)	1	6	256^3
X7=nF(232)	1	6	256^3

Table 2. Volume of Data Stored in VM

No. of Blocks (KB)	Stored Blocks in VM (MB)	Audio	Video	Text
0	5	80	600	20
0	100	60	500	20
5	200	10	125	10
10	400	8	100	5
20	600	6	75	3

The encoding matrix usually consists of a distinctiveness matrix and a Vander monde matrix or a Cauchy matrix. The performance of the matrix is high, provided the data blocks are of size c in mb. If the data blocks are less than the constant size c then we cannot combine with the existing encoding matrix. By following the rule, after every enciphering, the data blocks less than the constant c part of data blocks in upper server and the rest is stored in the poorer

server. Then, the blocks are stored individually in the local machine, cloud server and fog server By considering the most horrible case, even if the user is trying to filch data blocks, he cannot do so, because the data blocks are dispersed in various servers in different ratios based on the user defined assumption. So grouping the data blocks based on such assumption will not work accurately. The efficiency of the algorithm is, cent percent secured because, the author may not be given access to the encoded matrix value, which could be generated only by the valid user, on his own because, the degreee of difficulty is high due to the usage of Hash Solomon Code, which is used to segment the data into number of blocks.

Table 3. Comparative Storage Efficiency

No. of Blocks of Data used for Testing Efficiency	No. of Blocks in Tiang Wang Algorithm	No. of Blocks in Proposed System
0	0	0
0.5	0.5	0.525
0.6	5	5.25
0.75	7.5	7.875
0.79	10	10.5
0.8	12.5	19.125
0.85	15	15.75
0.89	17.5	18.375
0.89	20	21

Hence in **Table 3** acts as an evidence; improves the security and privacy by preventing, the stealer from accessing the segmented blocks of data. Efficiency of the above stated algorithm is evaluated based on the constant value c and size of the data blocks mb. Where X is Galos Field of Efficiency, and M is the repetitive block, and k is used to denote number of blocks after division by the whenever c = 3 mb and mb = 1, then the ratio for storing could be 20%. This has been depicted in **Fig. 3** as volume of data stored in terms of audio and video. Whenever we took the larger value for k then the efficiency of the algorithm will be more, based on the encryption and decryption value.

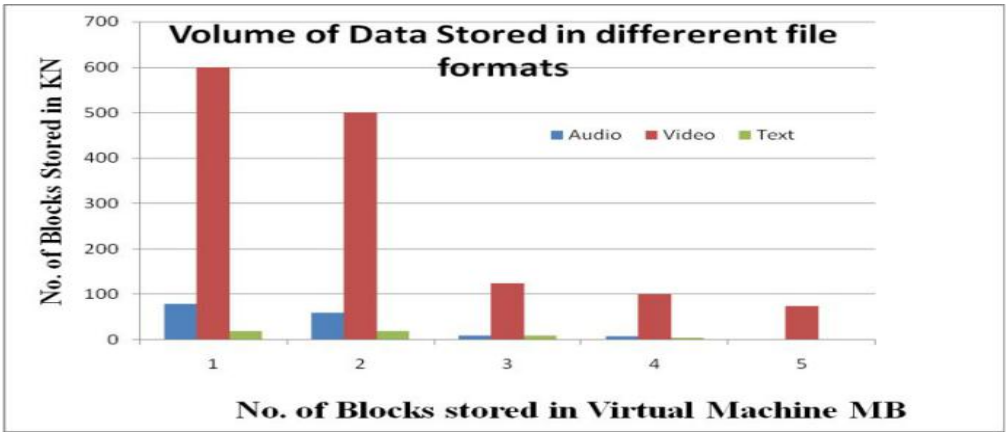

Fig. 3. Total Volume of data stored in user machine

The coding competency is associated to the Galois field. The association of ω, of the Galois field. Only when ω satisfies the relationship equation. The association of ω, c and mb satisfies the equation 2ϙ > c+mb. Whenever ω increases, the RAM will also get increases simultaneously. And also the efficient execution of the shared of ω can be represented by using **Table 3**. Hence, simultaneously. And also the efficient execution of the shared of ω can be represented by the algorithm for index efficiency helps to store more no of data blocks into cloud storage in an effective way. This has been depicted in the **Fig. 4** vey clearly. Even though the volume of data is huge in **Fig. 4** it accepts from the user and stores it, by splitting it into no of blocks, by locating it with the index no is an added flavor in this algorithm which reduces the complexity of the algorithm and improves the security in access.

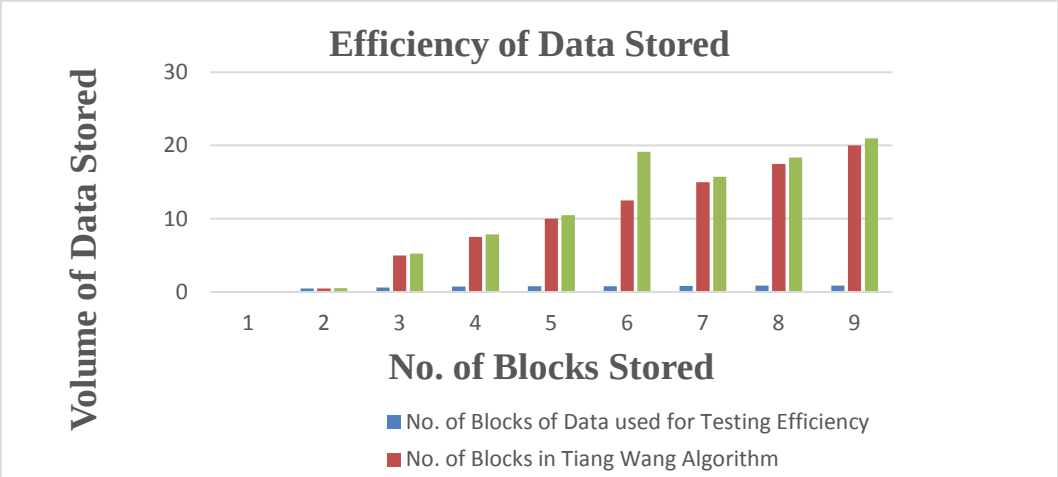

Fig. 4. Efficiency of data stored

6. Summary of Findings

The outcome of the performance analysis are summarised at place one for ease of understanding the contributions made by the FLRS preserving achieved in the present study.

They are as follows:-

1. Assign users the privilege of on-demand cloud storage services and obviates the need to be conscious of monitoring for data integrity.
2. A detailed security analysis demonstrates that the fourth layer enhances the preservation of data integrity against various forms of attacks. In addition, a comprehensive performance evaluation demonstrates that
3. All the four layers in an integrated and co-ordinated manner provides exclusive data security which is not only novel, yet feasible and efficient.
4. **Fig. 3** shows the relationship between audio, video and text data. In a dynamic storage approach the data gets stored based on distribution rate, immediately number of blocks (n) is calculated by keeping the block size of variable length (v), ways the block size is always incremented with (v+1.5).
5. This FLRS bridges the gap between the existing system TLS using Lamport in VMM.

The outcome of the performance analysis are summarised in one place for ease of understanding the contributions made by the FLRS preserving achieved in the present study. They are as implemented as block of size (v) increases storage at local host decrease its coercion. In case of encoding procedure if (v) increases (n) will grow exponentially to reduce the latency.

But during encoding, the cost of getting back the dispersed data consumes more time due to redundant number of blocks at second and third layers. All these computations are illustrated by taking constant to (n) as 2. **Fig. 2** shows the discrepancy in terms of time consumed for encoding procedure at second layer with that of decoding procedure of third layer in terms of time is shown in **Fig. 4**. VMM in which synchronizing the encoding and decoding procedure in distributed communication is achieved by introducing lamport algorithm by evading logical clock to synchronous the events.

The process of encoding/decoding may change at any time dynamically based on the size of block. So the indeterminate state should be given additional care keeping their record of entry through snapshot mechanism by using efficient indexing. The art of communication is tracked by assuming D is the process where I and j are the distributed channel then by following transit

$(LS_{ij},LS_{ij}) = ((EC_{ij}, SendMsg_{ij}),GTt)$ (1).

In similar way for decoding with acknowledge of indexing is generated transit

$(LS_{ij},LS_{ij}) = ((DC_{ij}, RecevedMsg_{ij}), GRTt)$. (2).

In between if the intruder is trying to decode the the data block will be tracked using cracking field of test to various block size restricted by through lamport algorithm.

7. Practical Implications

All procedures are used in real time in machine-to-machine communication, healthcare, professional sports, entertainment, business virtual augmented reality services, mission critical operations e.g., telesurgery, surveillance mapping which are the servicing areas of fog based computing. The clustered nodes does few services at reduced latency being nearer to the cloud server in the distributed environment play phenomenal role in IoT's.

The proposed FLRS using PPT and CI is an improvement over the three layered system now in vogue. The test results have validated its efficacy by enhancing the integrity along with higher security and better prevention against intrusion, compromised system software and data leakage. Further, provides better assurance to data controllers and analytic and machine learning IP developers that assert data is protected in deployment. In addition, ensures private sensitive data is accessed by only authorised software. Above all, it improves user's privacy and reduce cloud service provider's liability in the event of system compromise.

Even though it is not possible to crack the code, while using FLRSC, one of the limitations is that intruders may decode using matrix reverse tracking methodology. The evolving security techniques relies heavily upon emerging green computing. So, predictably it is better to provide effective resource restricted storage in cloud to begin with by using FLRS and difficulties can be overcome through the extention of this current work of green computing by adaptation.

To reduce the burden and storage cost of the devices in a structured way another successful point of extraction could be extented to indexing efficiency provided the logging user data structure is to be entered with proper records, and to be restricted to reverse hashing.

In the second classification phase, the accuracy of the KNN classifier was evaluated for test data. Leave-one-out cross-validation tests showed that this algorithm had a low error rate. The KNN classifier was found to have an error rate of about 2 percent for the test data, compared to an error rate of 7 percent for a MMD classifier. KNN is one of the simplest classification algorithms, but not necessarily the most accurate. Other supervised algorithms, such as back propagation (BP) and SVM, also have attractive features and should be compared in future work. It will be seen that the addition of a new layer (fourth layer) enhances the storage security in cloud environment.

8. Conclusions

The conventional storage technique by merely using encryption and decryption gave many limited benefits. However, users do not have control over the physical storage device in the cloud environment and suffers from security issues. Consequently, users may not have control over the physical storage device. The paper offers an original method of FLRS Scheme TLA constructed with hash Solomon code algorithm with inbuilt safety measures. The future work may be based on the ratio upon which the data are stored on to the cloud server/local server to ensure the security. Our FLRS approach is proven and feasible on deployment. Hence we can implement this in enhancing data security in IaaS under Cloud Architecture. In future work, as an extension to the present work, it is imperative to further explore efficient monitoring and validating mechanisms that are simpler, cost effective in the deployment of authentication challenge messages and algorithm so as to strike a judicious mix of storage, security, integrity, privacy and prevention from system compromise.

References

[1] Rajiv Ranjan, Massimo Villari, Haiying Shen, Omer Rana, Rajkumar Buyya, “Software tools and techniques fog and edge computing,” *Wiley sofware practice and experience Journal*, vol. 50, no. 5, pp. 473-475, March, 2020. Article (CrossRef Link)

[2] TianWang, WeijiaJia, XiZheng, GuojunWang, MandeXie, “Edge-based differential privacy computing for sensor–cloud systems,” *Elsevier Parallel and Distributed Computing Journal*, vol. 136, pp. 75-85, February 2020. Article (CrossRef Link)

[3] Ndikumana, N. H. Tran, D. H. Kim, K. T. Kim and C. S. Hong, "Deep Learning Based H. sed Caching for Self-Driving Cars in Multi-Access Edge Computing," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1-6, March 2020. Article (CrossRef Link)

[4] Mohammad Alibakhshikenari , Bal S. Virdee , Naser Ojaroudi Parchin, Panchamkumar Shukla Karim Quazzane, Chan H. See, Raed Abd-Alhameed, Francisco Falcone, Ernesto Limiti, "Isolation enhancement of densely packed array antennas with periodic MTM-photonic bandgap for SAR and MIMO systems," *IET Microwaves, Antennas & Propagation*, vol. 14, no. 3, pp. 183-188, February 2020. Article (CrossRef Link)

[5] J. Park, M. Rahman and H. N. Chen, "Isolation Enhancement of Wide-Band MIMO Array Antennas Utilizing Resistive Loading," *IEEE Access*, vol. 7, pp. 81020-81026, June 2019. Article (CrossRef Link)

[6] Mohammad Alibakhshikenari,Bal S. Virdee, P. Shukla, Chan H. See, RaedAbd-Alhameed, Francisco Falcone, and Ernesto Limiti, “Meta-Surface Wall Suppression of Mutual Coupling between Microstrip Patch Antenna Arrays for THz-Band Applications,” *Progress In Electromagnetics Research Letters*, vol. 75, pp. 105-111, May 2018. Article (CrossRef Link)

[7] Mohammad Alibakhshikenari, Bal Singh Virdeeband Ernesto Limiti, “Wideband planar array antenna based on SCRLH-TL forairborne synthetic aperture radar application,” *Journal of Electromagnetic Waves and Application*s, vol. 32, no.12, pp. 1586-1599, May 2018. Article (CrossRef Link)
[8] M. Alibakhshikenari, Bal S. Virdee, Chan Hwang See and Raed Abd-Alhame, "Wideband printed monopole antenna for application in wireless communication systems," *IET Microwaves, Antennas & Propagation*, vol. 12, no. 7, pp. 1222-1230, June 2018.
[9] Mohammad Alibakshikenari, Bal SVirdee, Abdul Ali, Ernesto Limiti “A novel monofilar-Archimedean metamaterial inspired leaky-wave antenna for scanning application for passive radar systems,” *Microw Opt Technol Lett*, vol. 60, no.8, pp. 2055-2060, June 2018. Article (CrossRef Link)
[10] Mohhammad Alibhakshikenari, Bal S.Virdee, Abdul Ali, Ernesto Limit, “Extended Aperture Miniature Antennar Based on CRLH Metamaterials for Wireless Communication Systems Operating Over UHF to C-Band," *Journal of Radio Science*, vol.52, no.2, 154-165, February 2018. Article (CrossRef Link)
[11] Mohhammad Alibhakshikenari, Ernesto Limit, et al., “A New Wideband Planar Antenna with Band-Notch Functionality at GPS, Bluetooth and WiFi Bands for Integration in Portable Wireless Systems,” *International Journal of Electronics and Communications*, vol.72, pp.79-85, February 2017. Article (CrossRef Link)
[12] Z. Zou, Y. Jin, P. Nevalainen, Y. Huan, J. Heikkonen and T. Westerlund, "Edge and Fog Computing Enabled AI for IoT-An Overview," in *Proc. of IEEE International Conference on Artificial Intelligence Circuits and Systems*, pp.51-56, 2019. Article (CrossRef Link)
[13] S. Saraswati H. P. Gupta and T. Dutta, "A Minimum Cost Real-Time Ubiquitous Computing System Using Edge-Fog-Cloud," in *Proc. of IEEE International Conference on Advanced Networks and elecommunications Systems*, pp.1-6, December 2018. Article (CrossRef Link)
[14] J. Liu, J. Weng, A. Yang, Y. Chen and X. Lin, "Enabling Efficient and Privacy-Preserving Aggregation Communication and Function Query for Fog Computing based Smart Grid," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 247-257, June 2019. Article (CrossRef Link)
[15] Nabil Abubaker, Leonard Dervishi, Erman Ayday, “Privacy-Preserving Fog Computing Paradigm,” in *Proc. of IEEE Workshop on CNS*, pp. 502-509, December 2017. Article (CrossRef Link)
[16] J Liang, Y. Long, Y. Mei, T. Wang and Q. Jin, “A Distributed Intelligent Hungarian Algorithm for Workload Balance in Sensor-Cloud Systems Based on Urban Fog Computing,” *IEEE Access*, vol. 7, pp. 77649-77658, June 2019. Article (CrossRef Link)
[17] Mehrzad Lavassani, Stefan Forsström, Ulf Jennehag, and Tingting Zhang, “Combining Fog Computing with Sensor Mode Machine Learning for Industrial IoT,” *Sensors*, vol. 18, no.5, pp. 1-20, May 2018. Article (CrossRef Link)
[18] K. Sangaiah, D. V. Medhane, T. Han, M. S. Hossain and G. Muhammad, "Enforcing Position-Based Confidentiality With Machine Learning Paradigm Through Mobile Edge Computing in Real-Time Industrial Informatics," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4189-4196, July 2019. Article (CrossRef Link)
[19] K. Sangaiah, D. V. Medhane, G. Bian, A. Ghoneim, M. Alrashoud and M. S. Hossain, "Energy-Aware Green Adversary Model for Cyberphysical Security in Industrial System," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3322-3329, May 2020. Article (CrossRef Link)
[20] K. Sangaiah, M. Sadeghilalimi, A. A. R. Hosseinabadi and W. Zhang, "Energy Consumption in Point-Coverage Wireless Sensor Networks via Bat Algorithm," *IEEE Access*, vol. 7, pp. 180258-180269, Novmber 2020. Article (CrossRef Link)
[21] Sangaiah, A.K. Hosseinabadi, A.A.R. Shareh, M.B., Bozorgi Rad, S.Y, Zolfagharian, A. Chilamkurti, N. IoT Resource Allocation and Optimization Based on Heuristic Algorithm,” *Sensors*, vol. 20, no. 2, pp. 1-26, January 2020. Article (CrossRef Link)

[22] .Mehrzad Lavassani, Stefan Forsström, Ulf Jennehag, and Tingting Zhang, "Combining Fog Computing with Sensor Mode Machine Learning for Industrial IoT," *Sensor*, vol.18, no.5, pp. 1-20, May 2018. Article (CrossRef Link)
[23] Maria Yuang, Po-Lung Tien, Wei-Zhang Ruan, Tien-Chien Lin, Shao-Chun, "OPTUNS: Optical intra-data center network architecture and prototype testbed for a 5G edge cloud [Invited]," *Journal of Optical Communications and Networking*, vol. 12, no. 1, pp.A28-A37, January 2020. Article (CrossRef Link)
[24] M. Bazm, M. Lacoste, M. Südholt and J. Menaud, "Secure Distributed Computing on Untrusted Fog Infrastructures Using Trusted Linux Containers," in *Proc. of IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Nicosia*, pp.239-242, Dec.2018. Article (CrossRef Link)
[25] L. Zhou, L. Yu, S. Du, H. Zhu and C. Chen, "Achieving Differentially Private Location Privacy in Edge-Assistant Connected Vehicles," *IEEE Internet of Things Journal*, vol.6, no.3, pp. 4472-4481, June 2019. Article (CrossRef Link)
[26] Zhou, T. Wang, M. Z. A. Bhuiyan and A. Liu, "A Hierarchic Secure Cloud Storage Scheme Based on Fog Computing," in *Proc. of 5th IEEE Intl Conf on Dependable, Autonomic and Secure Computing*, pp.470-477, November 2017. Article (CrossRef Link)
[27] W. Abdul, Z. Ali, S. Ghouzali, B. Alfawaz, G. Muhammad and M. S. Hossain, "Biometric Security Through Visual Encryption for Fog Edge Computing," *IEEE Access*, vol. 5, pp. 5531-5538, Apr.2017. Article (CrossRef Link)
[28] Tian Wang , Jiyuan Zhou, Anfeng Liu, and Md Zakirul Alam Bhuiyan, "Fog-Based Computing and Storage Offloading for Data Synchronization in IoT," *IEEE Internet of Things Journal*, vol.6, no.3, pp. 4272-4282, June 2019. Article (CrossRef Link)
[29] S. N. Shirazi, A. Gouglidis, A. Farshad and D. Hutchison, "The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog from a Security and Resilience Perspective," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2586-2595, November 2017. Article (CrossRef Link).

Nirmala E is currently pursuing Ph.D. in the research area of Cloud Computing and Security at the Department of Computer Technology, Madras Institute of Technology, Anna University Campus, Chennai, India under the guidance of Dr.S.Muthurajkumar, Department of Computer Technology, M.I.T, Anna University Campus. Nirmala completed her M.C.A. in University of Madras and M.E. from St.Peter's University, She has over 16 years of teaching experience; published 2 papers in International journal and conference. Her areas of interest are Cryptography, Security in cloud computing and Block Chaining.

Dr.Muthurajkumar S, Assistant Professor, Department of Computer Technology, Anna University, Chennai 600 044 from December-2014. His areas of interest are Cloud Computing, DBMS, Data Structures, Computer Architecture and Digital Systems. He has to his credit 26 papers published in various International/ National Journals and also presented 4 Research Papers in International programmes and one in National Program. He has attended assorted workshops, Faculty Development programmes and seminars held at engineering colleges