iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35445

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Efficient Local Secret Sharing for Distributed Blockchain Systems

G. Latha[1], SK. Allabi[2], M. Prathyusha[3], K. Suresh[4]
[1]*Associate Professor,* [2, 3, 4]*Student, Department of Computer Science and Engineering, CMR Technical Campus, Medchal, Hyderabad, Telangana, India*

Abstract: ***Blockchain system store transaction data in the form of a distributed database where each peer is to maintain an identical copy. Blockchain systems resemble repetition codes, incurring high storage cost. Recently, distributed storage blockchain (DSB) systems have been proposed to improve storage efficiency by incorporating secret sharing, private key encryption, and information dispersal algorithms. However, the DSB results in significant communication cost when peer failures occur due to denial of service attacks. In this project, we propose a new DSB approach based on a local secret sharing (LSS) scheme with a hierarchical secret structure of one global secret node and several local secret nodes. The proposed DSB approach with LSS improves the storage and recovery communication costs.***
Keywords: Distributed Storage Blockchain (DSB) Local Secret Sharing (LSS) Shamir Secret Key(Algorithm)

I. INTRODUCTION

The project titled "Efficient Local Secret Sharing for Distributed Blockchain System's" scope is to store data efficiently and to secure data from attacks. In this we use DSB approach based on a local secret sharing (LSS) scheme. LSS efficiently incorporates local secrets and global secrets into a hierarchical secret sharing scheme Networks for this purpose. To reduce storage space Distributed Blockchain storage was introduced where all nodes will share a part of data instead of storing entire data or keys by using SHAMIR SECRET KEY algorithm

II. EXISTING SOLUTION AND ITS DRAWBACKS:

In existing Blockchain system each node was storing complete data '527166' but in distributed Blockchain each node will store only its share such as 52 in one node and attack or down then we cannot get it share and we cannot reconstruct original data and to reconstruct original data distributed nodes has to find out all nodes who have this shares which can cause lots of communication cost.

A. *Disadvantage*

1) Security issues are more.
2) Need more storage space
3) Cost of recovery is more
4) Chances for loss of data

III. PROPOSED SYSTEM AND ADVANTAGES:

In this paper ,we introduce Local Secret Sharing (LSS) where hash code will be consider as common data which require by all node for verification so hash code will be strore as GLOBAL private keys will be consider as local data and not require by all nodes so it connecting to local nodes. So in propose work hash code and private keys will store in different LOCAL and GLOBAL nodes so storage cost will be some more reduce and node can recover data from its local neighbours. so communication cost will also be reduced

A. *Advantages*

1) Security is more
2) No Loss of data
3) Low Cost
4) Cost of recovery is less

IV. SYSTEM ARCHITECTURE

The system architecture shows the procedure followed for Efficient Local Secret Sharing for Blockchain Systems.

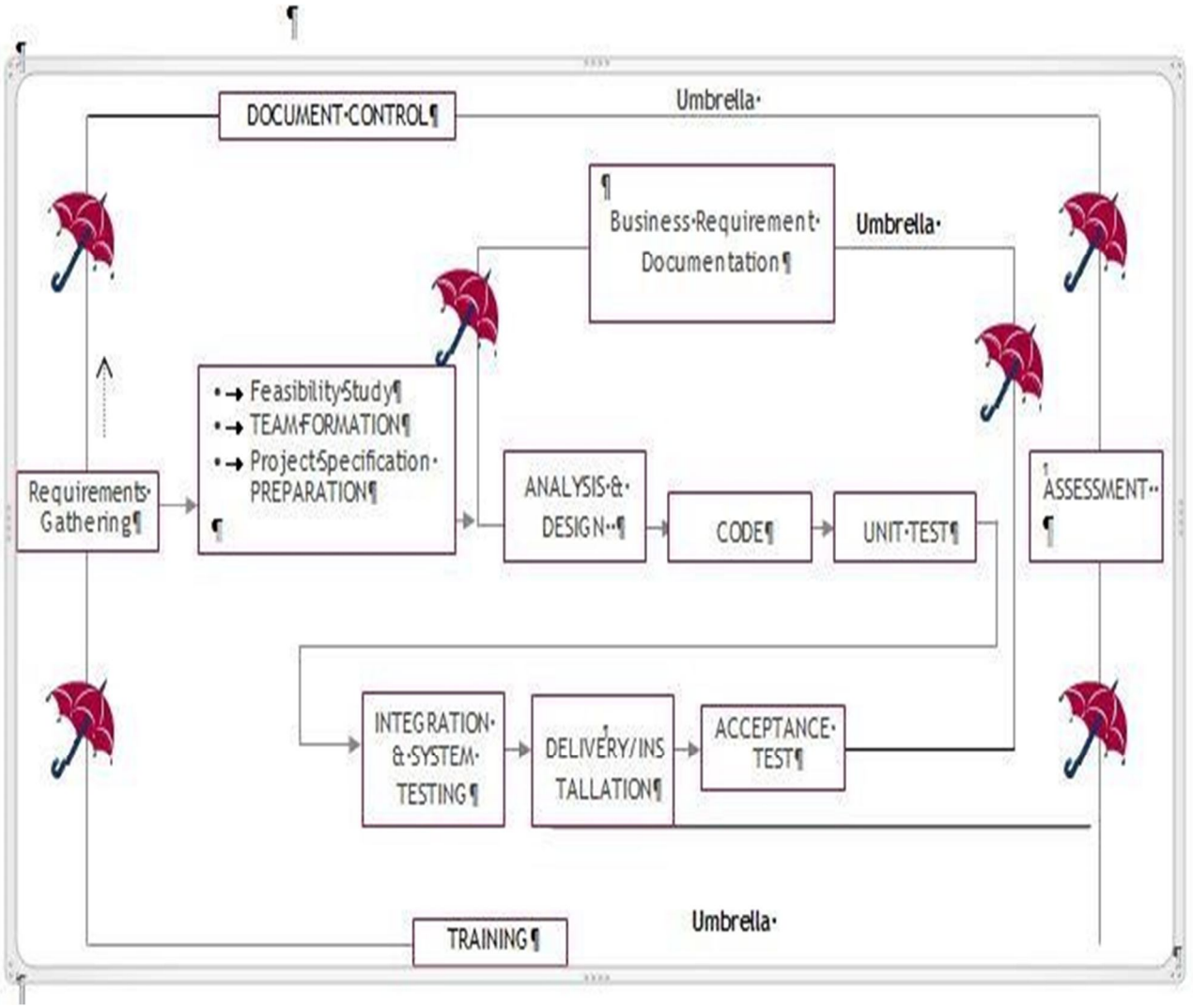
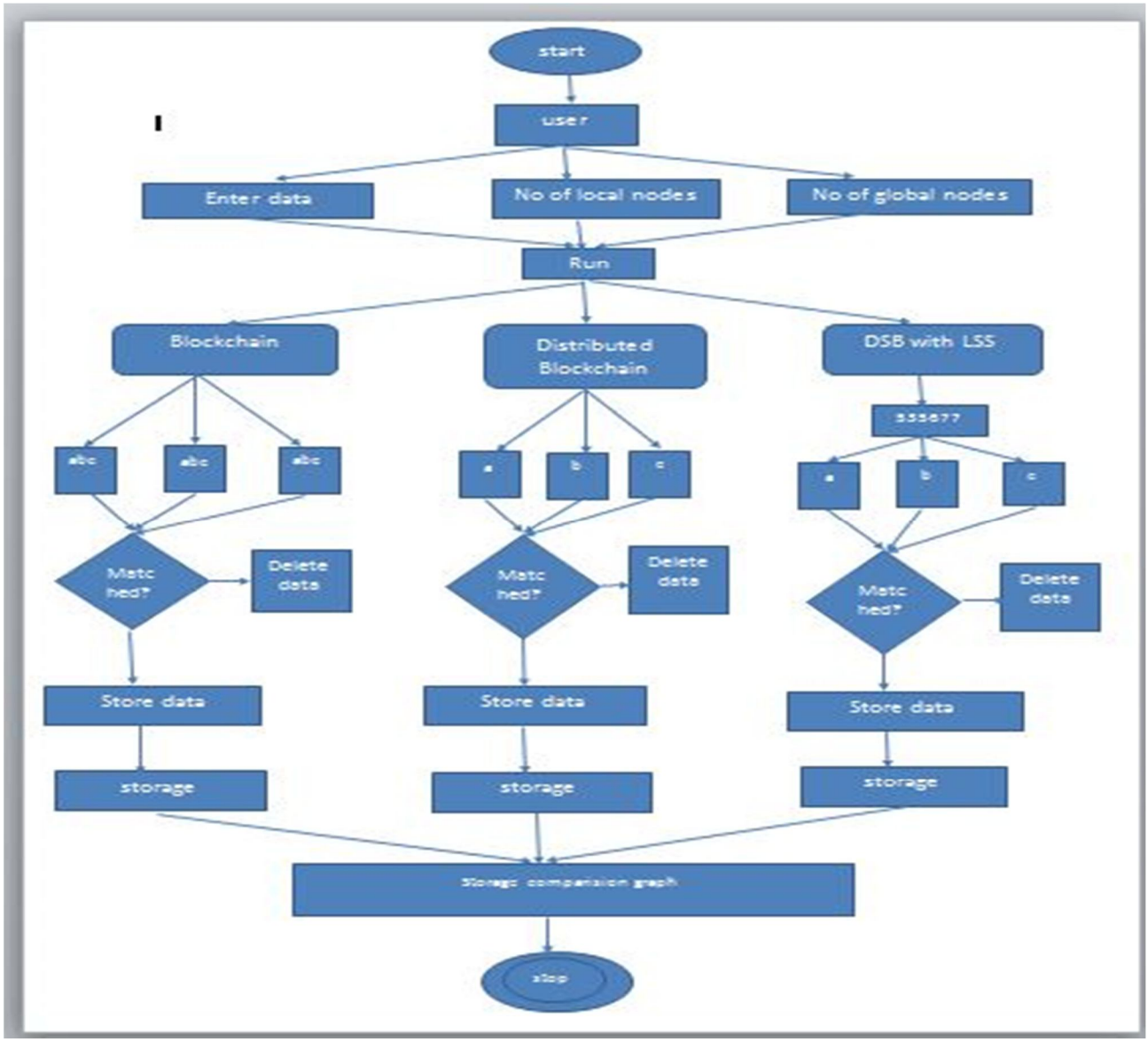


Fig1:Project Architecture of efficient local secret sharing for distributed blockchain systems.

A. Modules

1) *Enter Data:* The Enter Data is the initial module in our project In this we have to enter some data to encrypt and to store in blockchain.
2) *Number Of Local And Global Peers:* Then enter number of global peers to store hash code and then local peers will store private keys share.
3) *Run Traditional Blockchain:* In traditional Blockchain we don't have any secret sharinh scheme so we are not showing any data related to sharing
4) *Run Distributed Storage Blockchain (DSB):* The Distributed Storage Blockchain is one of the module in our project.After run the DSB in the screen we get selected text first showing previous and Current block hash codes and then displaying encrypted data then displaying decrypted data with the help of private keys and then displaying DSB storage cost.
5) *Run Distributed Storage Blockchain with LSS:* Run Distributed Storage Blockchain with LSS to share secret hash code in global peer and private keys in local peers and then calculate storage cost
6) *Storage Comparision Graph:* In storage Comparision Graph x-axis represents technique name and y-axis represents storage cost for each technique.

B. Process Flow Diagram



C. Algorithm

Given partition $\mathcal{A} = \{A_1, \ldots, A_{\frac{n}{r+1}}\}$:

1: Set hash value $W^{(t)}$ as global secret $s^{(t)} = a_{0,0} \in \mathbb{F}_q$.
2: Generate a random vector $\mathbf{a}^{(t)}_{\setminus a_{0,0}} \in \mathbb{F}_q^{k-1}$.
3: Compute local secrets $s_l^{(t)}$ for $l \in [1, \frac{n}{r+1}]$ and $(f_{\mathbf{a}}^{(t)}(\alpha_i))$ for $i \in [1, n]$ by Alg. 2.
4: Distribute and store $(f_{\mathbf{a}}^{(t)}(\alpha_i))$ into n peers.
5: **for** $l = 1$ to $\frac{n}{r+1}$ **do**
6: Encrypt $B^{(t)}$ with $s_l^{(t)}$ as $\mathbf{m}_l^{(t)} = \Phi(B^{(t)}; s_l^{(t)})$.
7: Encode $\mathbf{m}_l^{(t)}$ into $\mathbf{c}_l^{(t)}$ by $(r+1, r)$ coding.
8: Distribute and store $\mathbf{c}_l^{(t)}$ among peers in A_l.
9: **end for**

V. LITERATURE SURVEY

On scaling decentralized blockchains the increasing popularity of blockchain based cryptocurrencies has made scalability a primary and urgent concern.

A. *"How to Share a Secret,*

In this paper we show how to divide data D into n pieces pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of k - 1 pieces reveals absolutely no information about D. This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces

B. *"A Family of optimal locally Recoverable Codes,"*

A code over a finite alphabet is called locally recoverable (LRC) if every symbol in the encoding is a function of a small number (at most r) other symbols. We present a family of LRC codes that attain the maximum possible value of the distance for a given locality parameter and code cardinality

C. *"Efficient Multicast Packet Authentication,"*

We describe a novel method for authenticating multicast packets that is robust against packet loss. Our main focus is to minimize the size of the communication overhead required to authenticate the packets. Our approach is to encode the hash values and the signatures with Rabin's Information Dispersal Algorithm (IDA) to construct an authentication scheme that amortizes a single signature operation over multiple packets. This strategy is especially efficient in terms of space overhead, because just the essential elements needed for authentication (i.e., one hash per packet and one signature per group of packets) are used in conjunction with an erasure code that is space optimal. To evaluate the performance of our scheme, we compare our technique with four other previously proposed schemes using with four other previously proposed schemes using analytical and empirical results Two different bursty loss models are considered in the analysis.

VI. RESULT ANALYSIS

We will compare the storage of Traditional Blockchain, Distributed Blockchain and Distributed Blockchain with Local secret Sharing

A. *Traditional Blockchain Storage*

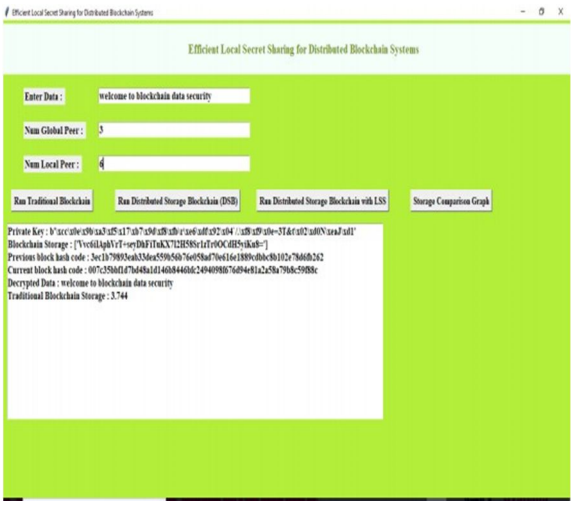


Fig2:Traditional Blockchain storage

In above screen first output line showing generated private key and second line showing encrypted data store in Blockchain and 3rd and 4th line represents previous and current block hash code and 5h line represents decrypted data and in 6th line displaying storage space as 3.744 KB to store all data accuracy compare to all other algorithm.

B. Distributed Blockchain Storage (DSB)

In above screen in selected second row while decrypted we collected all data and then combining all data to reconstruct original private key and in above screen reconstructed original private key is 420127.

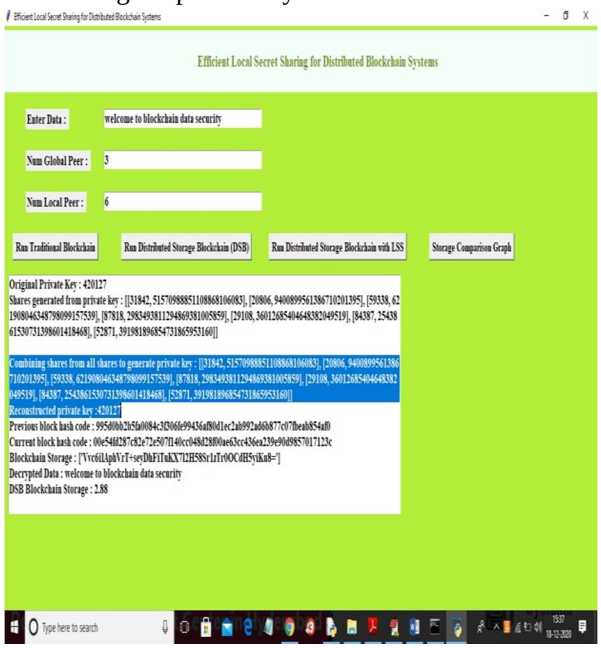


Fig -3 Distributed Blockchain Storage

C. DSB with Local Secret Sharing Storage

Fig4: DSB with LSS storage

In above screen also we will get same output as DSB but the only difference is instead of storing private and hash code in all nodes we have store hash code in all nodes we have store hash code in global nodes and private keys in local nodes and due to separation of hash code and private keys the storage space will be reduce and upon node failure they can recover data just by connecting with their local neighbours instead of connecting to all nodes and can save communication cost also Now click on 'Storage Comparison Graph' button to get below screen

D. Storage Comparision Graph

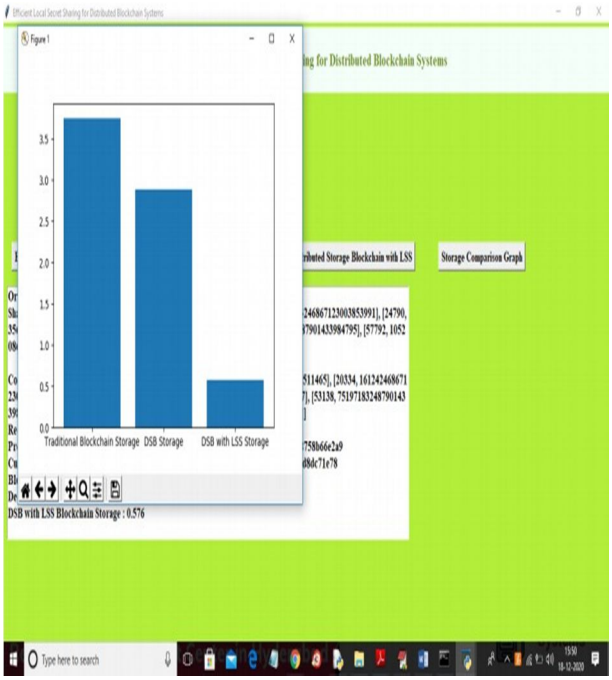


Fig5:Storage Comparision Graph

In above graph x-axis represents technique name and y-axis represents storage cost for each technique and from above graph we can conclude that DSB with LSS consume less storage space compare to all other techniques.

VII. CONCLUSION

In this letter, we have proposed a new DSB scheme based on LSS. The proposed scheme improves the storage and recovery communication costs. The extensions of the LSS to more general frameworks would be interesting for further future topics

VIII. FUTURE SCOPE

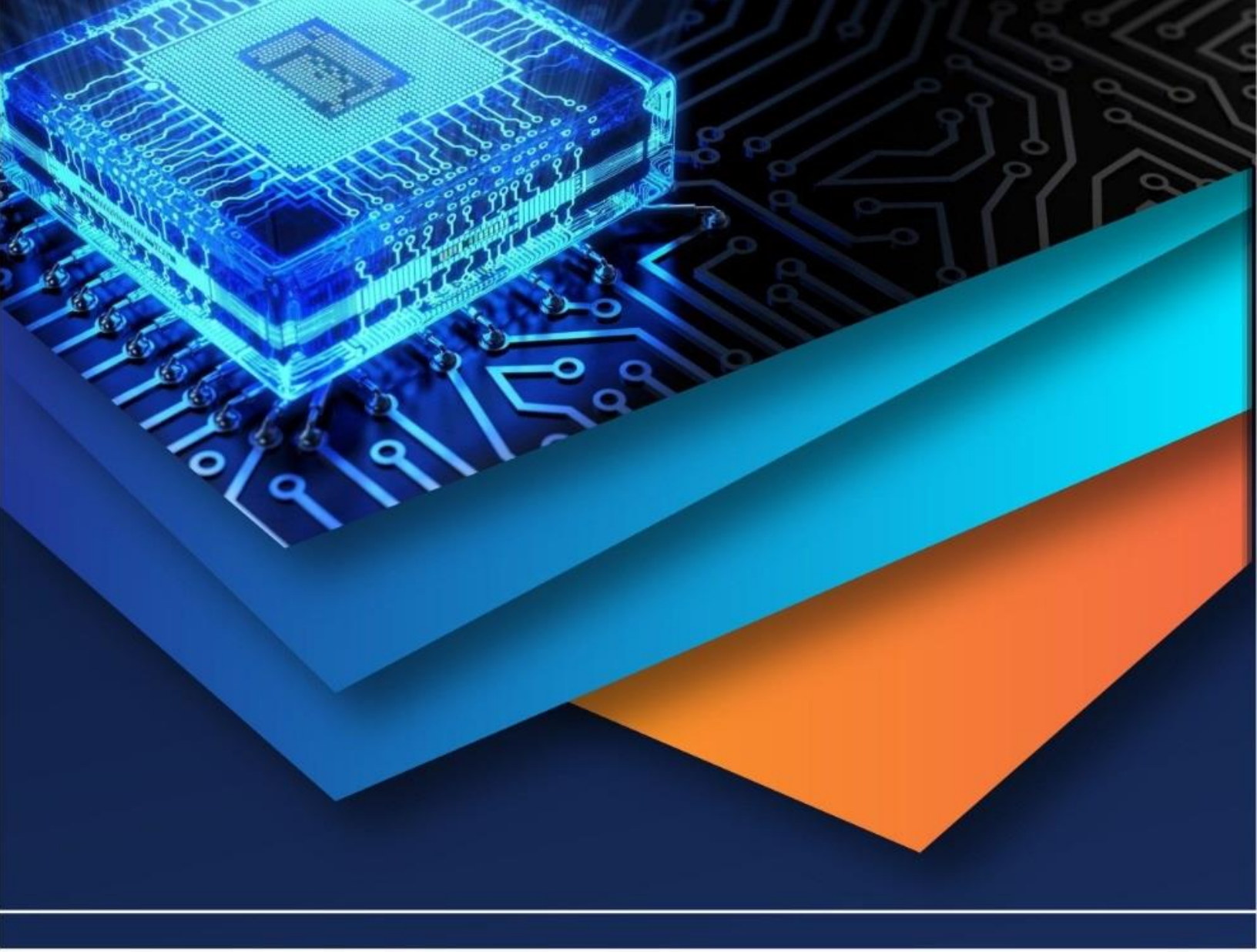
The proposed scheme improves the storage and recovery communication costs. The extensions of the LSS to more general frameworks would be interesting for further future topics. Our belief is that research students will use this paper as a spring board for doing qualitative research in spam filtering using machine learning, deep leaning and deep adversarial learning algorithms.

IX. ACKNOWLEDGEMENT

The authors would like to acknowledge the support of the Chairman, Director and Head of the Department, Department of Computer Science and Engineering, CMR Technical Campus, Medchal, Hyderabad, Telangana for their encouragement to the authors.

REFERENCES

[1] K. Croman et al., “On scaling decentralized blockchains,” in Proc. Int. Conf. Financial Cryptogr. Data Secur., Aug. 2016, pp. 106–125.
[2] R. K. Raman and L. R. Varshney, “Distributed storage meets secret sharing on the blockchain,” in Proc. Inf. Theory Appl. Workshop (ITA), Feb. 2018.
[3] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612– 613
[4] A. Pannetrat and R. Molva, “Efficient multicast packet authentication,” in Proc. Netw. Distrib. Syst.security symp.
[5] A. Pannetrat and R. Molva, “Efficient multicast packet authentication,” in Proc. Netw. Distrib. Syst. Security Symp. (NDSS), Feb. 2003
[6] R. K. Raman and L. R. Varshney, “Dynamic distributed storage for blockchains,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2018, pp. 2619–2623. [Online]. Available: https://arvix.org/pdf/1711.07617.pdf
[7] H.Krawczyk, “Secret sharing made short,” in Proc. Annu. Int. Cryptol. Conf., Jan. 1994, pp. 136–146.
[8] M. O. Rabin, “Efficient dispersal of information for security, load balancing, and fault ,” J. ACM, vol. 36, no. 2, pp. 335–348, Apr. 1989.
[9] I. Tamo and A. Barg, “A family of optimal locally recoverable codes,” IEEE Trans. Inf. Theory,vol.60, no.8,pp.4661 Aug.2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY