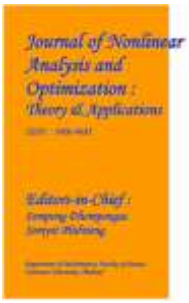
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 2 : 2024
ISSN : **1906-9685**



Smart Integrity Checks: Keeping Cloud Data Safe with Keyword-Based Auditing and Privacy Protection

1K. Jaya Krishna, 2Yeruva Venkata Reddy,

1Associate Professor, Department of Master of Computer Applications, QIS College of Engineering & Technology, Ongole, Andhra Pradesh, India

2PG Scholar, Department of Master of Computer Applications, QIS College of Engineering &Technology, Ongole, Andhra Pradesh, India

ABSTRACT

Mobile cloud storage (MCS) provides clients with convenient cloud storage service. In this paper, we propose an efficient, secure and privacy-preserving mobile cloud storage scheme, which protects the data confidentiality and privacy simultaneously, especially the access pattern. Specifically, we propose an oblivious selection and update (OSU) protocol as the underlying primitive of the proposed mobile cloud storage scheme. OSU is based on onion additively homo morphic encryption with constant encryption layers and enables the client to obliviously retrieve anencrypted data item from the cloud and update it with a fresh value by generating a small encrypted vector, which significantly reduces the client's computation as well as the communication overheads. Compared with previous works, our presented work has valuable properties, such as fine-grained data structure (small item size), light weight client-side computation (a few of additively homo morphic operations) and constant communication overhead, which make it more suitable for MCS scenario. Moreover, by employing the "verification chunks" method, our scheme can be verifiable to resist malicious cloud. The comparison and evaluation indicate that our scheme is more efficient than existing oblivious storage solutions with the aspects of client and cloud workloads, respectively.

Index: mcs, osummorphic encryption, cloudstorage

I. INTRODUCTION

IN mobile cloud storage (MCS), data is stored on a cloud and can be accessed from anywhere with mobile devices. Due to the attractive properties, MCS is becoming more and more popular. Some large companies provide MCS services for business purposes, i.e. Apple I Cloud, Drop box, Microsoft One Drive and Google Drive. In many situations, the cloud is not considered fully trusted. Thus, the client may employ encryption schemes to keep data confidential before uploading it to the cloud. However, in MSC-based applications, data always be related to

certain information, such as location information in location based services. In this situation, which item of data is being accessed leaks addition information to the cloud server. By utilizing this leaked information of access pattern, the cloud may infer the operation of the client and even the content of the encrypted data. For example, in a searchable encryption system, a cloudcan identify approximately 80% of the search queries by applying a general inference attack with access pattern leakage and minimal background knowledge [1]. Oblivious technology, such as oblivious transfer (OT) [2], oblivious storage (OS) [3]and oblivious random access machine (ORAM) [4], is a kind of technology that can protect both data and access pattern. Generally speaking, these

technologies allow a client to access its outsourced data stored in an un trusted cloud without revealingwhich items have been visited or even what kinds of operations are requested. Due to the high level privacy preservation, these technologies have been widely applied in various application scenarios such as searchable encryption [5][7], encrypted hidden volumes [8], [9], cloud storage [10][13], multi-party computation [14][18], etc. However, there are some challenges to employ existing oblivious schemes into MCS scenario due to several reasons. Firstly, mobile devices are generally connected to the Internet via wireless networks, such as ad-hoc, LTE, and Wi-Fi. That means the mobile devices have limited communication bandwidth to download and upload data. Thus, some schemes suffered by the well- known communication bandwidth overhead lower bound result O (log N) cannot be employed into MCS due to the heavy communication overhead. 1 Secondly, although modern mobile devices, such as mobile phones and tablets, have significantly improvement in terms of computing capability, they still cannot compete with personal computers or other powerful devices. Complicated computation also reduces the battery life of mobile devices. Therefore, some schemes based on fully homomorphic encryption (FHE) [19] or multi-layer onion additively homomorphic encryption [20] are also not suitable for MCS due to complex client- side encryption and decryption computation, although they circumvent the communication lower bound and achieve constant communication bandwidth overhead. Thirdly, many existing oblivious schemesare also suffered by the lager minimum effective item size. Minimum effective item size refers to the minimal number of bits in aneffective item of an oblivious scheme required to meet the predefined communication complexity (constant or logarithmic). Lager item size prevents the mobile client from fine-grained accessing its own data. Moreover, it also further increases the communication or computation overhead of existing oblivious schemes.

Some oblivious schemes consider to introduce data locality to improve efficiency. Data locality reveals the tendency of a client to access its data over a short time. Spatial locality and temporal locality are two typical types of

reference locality of data access. Spatial locality refers that the client may access the nearby data items if a particular item is accessed. Temporal locality refers that the client will reuse data repeatedly within a short time. By taking spatial locality into consideration in non- constant communication overhead oblivious schemes, the amortized communication overhead whiling accessing a series of items is lower than that whiling accessing one item independently [21]. Taking advantage of temporal locality can also significantly improve efficiency of particular oblivious schemes since if an item is visited, it only requires lightweight computation and communication to access the item again in a short time. However, as far as we know, there is no related work that has considered temporal locality. In this paper, we propose an efficient, secure and privacy-preserving mobile cloud storage scheme. The proposed scheme has the following properties:

1) protecting data confidentiality and access patternsimultaneously,

2) constant communication bandwidth overhead,

3) low client side computation (a few additively homomorphic encryption and decryption operations),

4) small minimum effective item size (several kilobytes for reasonable data capacity),

5) taking temporal locality into consideration, and

6) verifiable (against malicious cloud). Specifically, we highlight our contributions of thispaper in the following. We define a two-party protocol, i.e. oblivious selection and update (OSU) protocol, and present a concrete construction of OSU protocol. OSU allows a client to obliviously retrieve its encrypted data from the cloud and update the data with a fresh value. Compared with other methods, such as PIR-Read combined PIR- Write, OSU requires less communication and client computation. For particular data size, the proposed OSU has O (1) communication complexity andrequires the client to execute minimum encryption and decryption operations. Moreover, the protocol is of independent interest for other secure multi- party computation application scenarios.Based on the proposed OSU protocol, we present an efficient, secure and privacy-preserving mobile cloud storage scheme. The scheme can simultaneously protect data content and preserve access pattern privacy. Compared with previous works, our scheme has small item size, low client-side computation, and constant communication overhead. We also introduce temporal locality into our construction to further enhance the efficiency. By combining “verification chunks” method, our scheme can be verifiable and resist malicious cloud. Furthermore, we evaluate our construction and other related works and the experimental performances show that our scheme is more efficient.Organization. The remainder of the paper is organized as follows: In Section 2, we review some related works. In Section 3, we introduce the system model and threat model of the mobile cloud storage. The preliminaries as well as the oblivious selection and update protocol are described in Section 4. Our

proposed mobile cloud storage scheme and the proofs and analyses are introduced in Section 5 and6, respectively. Finally, we give the evaluation and conclusion in Section 7 and 8.

II. LITERATURE SURVEY

1.TITLE : A Secure Searchable Encryption Framework for Privacy Critical Cloud Storage Services

Year: March 2021

Authors: Boda Sai Sree G.Natraj Shekhar, Kiran Kumar Mungara

Abstract: SSE was first presented by Song et al. Curtmola etal. proposed a sub direct SSE conspire and presented the security idea for SSE called versatile protection from picked catchphrase assaults (CKA2). Refinements of have been proposed which offer broadeneds functionalitis[11]. In any case, the static idea of those plans restricted their relevance to applications that require dynamic document assortments. Kamara et al. were among the first to build up a DSSE conspire in that could deal with dynamic record assortments by means of ascrambled list. Not with standing, it releases huge data for updatesand it isn't parallelizable.

Kamara et al. proposed a DSSE plot, which released less data than that of and it was parallelizable. As of late, a progression of new DSSE plans have been proposed which offer different compromises between security, usefulness and effectiveness properties like little spillage, adaptable quests with broadened inquiry, or high productivity.Enlivened by the work from Kamara proposed another sub direct DSSE plot which underpins more intricate questions like disjunctive and boolean inquiries.

2.TITLE: A Three Layer Privacy Preserving Cloud Storage Scheme BasedOn ComputationalIntelligence in Fog Computing

Year: May 2021

Author: Vaspari Kalyani,B.Suresh , K.Anjaneyulu , K.Krishna

Abstract: The meaning of security in circulated capacity has pulled in a lot of thought paying little heed to in academe or industry. There areahuge load of examines about secure circulated stockpiling structures of late. To settle the security issue in conveyed processing, paper proposed an insurance saving and copy anticipation BIR plot using encryption and watermarking methodology. This arrangement can get the image substance and pictures incorporates well from the semi-genuine cloud laborer, and keep the image customer from unlawfully passing on the recuperated pictures. Shenet al. think cloud is semi-trusted and propose a framework for metropolitan data sharing by mishandling the qualitybased cryptography. The arrangement they proposed is get and can contradict possible attacks. Fuet al. propose a substance careful chase plot, which canmake semantic request more insightful.The examinations results show that their arrangement is compelling, Hou, Pu and Fan consider that in customary condition, customer's data is takencare of through CSP, whether or not CSP is dependable, aggressors can regardless get customer's data if they control the dispersed stockpiling the heads center point. To dodge this issue, they propose an encoded file structure

dependent on an unbalanced test reaction confirmation component. So they propose a safe virtual protection plot reliant on SSL and Daoli moving data over SSL and sending Daoli on the cloud laborer, the system scrambles data before it isformed into the hard circle. Feng brings up, the weight of worker will increment and information may spill during transmission in cloud workers. Feng proposes a more succinct plan: scrambling information in shut cloud climate.

3. TITLE: A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage

Year: August 2021

Authors: Areddy Priyanka, T Baba, Kiran Kumar Mungara

Abstract: Software solutions always provide a dynamic environment where business and technology strategies converge. The very different approach focuses on new ways of business combining IT innovation and adoption while also leveraging an organization's current IT assets. Nowa days it is spreading and work with large global corporations and new products or services and to implement prudent business and technology strategies in today's environment

III. PROBLEM STATEMENT

Goldreich and Ostrovsky introduced the first concept, oblivious randomaccess machine (ORAM), to preserve access pattern privacy [4]. They proposed a concrete solution, Square Root ORAM, and demonstrated a communication overhead lower-bound blowup (logN). In their setting (passive setting), the memory, or cloud in cloud computing application, acted as a passive storage entity and does not execute any computation on data. Under this setting, a series of works had been improved in terms of theory and efficiency [22]– [33]. Shi et al. first organized their construction into a binary tree over buckets [24].

By operating blocks along tree paths, the proposed construction achieved O (log3 N) communication worst-case cost. Path ORAM [26] was proposed by Stefanov et al. based upon the binary tree ORAM framework. It achieved the (logN) lower-bound blowup demonstrated by Goldreich and Ostrovsky

[4] in passive setting. It was also extremely simpler than other constructions by avoiding using complicated cryptographic primitives and efficient with small end-to-end delay for reasonable parameters.

Actually, the current cloud is considered to have significant computational resource and can execute heavy computation. A series of subsequent works followed the computation cloud setting and circumvent the lower-bound by allowing the cloud to execute heavy computation for the client [19], [20], [34]. Although it was not the first one to adopt cloud computation model, Apon et al. first formalized the verifiable oblivious storage, which generalizes the notion of ORAM by allowing the storage medium to perform computation [19].

Devadas et al. proposed a constant communication bandwidth ORAM, i.e. Onion ORAM, with cloud computation [20]. In Onion ORAM, data blocks were encrypted under multi-layer (forming as an "onion") additively homomorphic encryption scheme [35] or

alternatively somewhat homomorphic encryption scheme [36], which allowed the client to retrieve the target blocks and evict blocks through paths with small encrypted select vectors. By combining the reverse lexicographical eviction order method [16], OnionORAM overflowed with negligible probability for eligible security parameters. Moataz et al. proposed another constant communication bandwidth ORAM named C-ORAM [34]. Compared with Onion ORAM, C-ORAM removed layeredhomomorphic encryption and replaced it with an efficient oblivious merging technique.

3.1 Disadvantages

1. An existing methodology doesn't implement Additively Homomorphic Encryption method.
2. The system not implemented Resistance to Malicious Cloud Concept.

IV PROPOSED SYSTEM

In this paper, we propose an efficient, secure and privacy-preserving mobile cloud storage scheme. The proposed scheme has the following properties:

1) protecting data confidentiality and access patternsimultaneously,
2) constant communication bandwidth overhead,
3) low clientside computation (a few additively homomorphic encryption and decryption operations),
4) small minimum effective item size (several kilobytes for reasonable data capacity)
5) taking temporal locality into consideration, and
6) verifiable (against malicious cloud). Specifically, we highlight our contributions of thispaper in the following.

We define a two-party protocol, i.e. oblivious selection and update (OSU) protocol, and present a concrete construction of OSU protocol. OSU allows a client to obliviously retrieve its encrypteddata from the cloud and update the data with a freshvalue. Compared with other methods, such as PIR- Read combined PIR-Write, OSU requires less communication and client computation. For particular data size, the proposed OSU has O(1) communication complexity and requires the client to execute minimum encryption and decryption operations. Moreover, the protocol is of independent interest for other secure multi-party computation application scenarios. Based on the proposed OSU protocol, we present an efficient, secure and privacy-preserving mobile cloud storage scheme. The scheme can simultaneously protect data content and preserve access pattern privacy. Compared with previous works, our scheme has small item size, low client-side computation, and constant communication overhead. We also introduce temporal locality into our construction to further enhance the efficiency. By combining "verification chunks" method, our scheme can be verifiable and resist malicious cloud. Furthermore, we evaluate our construction and other related works and the experimental performances show that our scheme is more efficient.

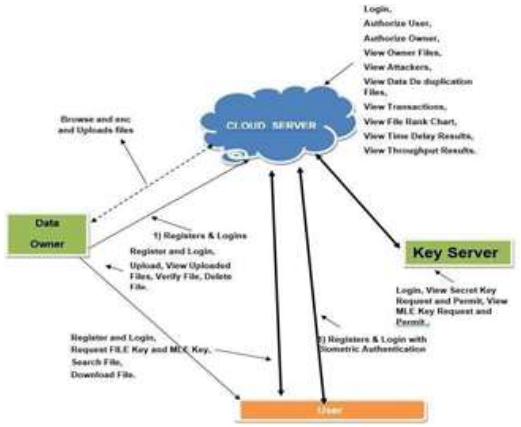
4.1 Advantages

1. Additively Homomorphic Encryption which is a form of public key encryption. It allows anyone

with the public key to manipulate ciphertexts to generate a new ciphertext, which is encrypted of corresponding operation result of original plaintexts.

2.The proposed system is more efficient, secure, and privacy preserving mobile cloud storage scheme, which is suitable for lightweight application and against malicious cloud server.

V. SYSTEM ARCHITECTURE



System architecture is the process of designing theelements of a system such as the architecture, modules, and components, the different interfaces of those components, and the data that goes throughthat system.

VI. METHODOLOGY

6.1 Data Owners

In this module, the data provider uploads their encrypted Owners data in the Cloud server. For thesecurity purpose the user encrypts the data file and then store in the server. The User can have capable of manipulating the encrypted data file and performs the following operations Register and Login, Upload Blocks, Verify Block (Data Auditing), Update Block, Delete File, View Uploaded Blocks.

6.2 Cloud Server

The Cloud server manages which is to provide data storage service for the Data Owners.Data owners encrypt their data files and store them in the Server for sharing with data consumers and performs the following operations such as Login, View DataOwners, View End Users, View Hash Table, View File Request, View Transactions, View Attackers, View Results, View File Time Delay Results, ViewFile Throughput Results.

6.3 End User

In this module, the user can only access the data file with the secret key. The user can search the file fora specified keyword and end user and can do the following operations like Register and Login, View All Data Owner Files, Request File, View File Response, Download File.

6.4 Auditor

In this module, the key issuer performs the following operations Login, View Hash Table, View Attackers, View File Updated or Deleted, View Results.

VII. ALGORITHMS

Algorithm 1 Setup

Input: The file set F.
Output: The encrypted data block set C, the keyword set W, the index vector set V, the secret key x and the public key y.

for each $F_i \in F (1 \le i \le n)$ **do**
  Split it into s blocks $F_{i1}, F_{i2}, ..., F_{is}$;
  for each $1 \le j \le s$ **do**
    Compute $c_{ij} = Enc(F_{ij}, k_0)$;
  end for
end for
Set $C = \{c_{ij}\}(1 \le i \le n, 1 \le j \le s)$;
Extract all keywords, and build W;
for each $w_k \in W (1 \le k \le m)$ **do**;
  Create an $n - bit$ binary string v_{w_k};
  Initiate all elements in v_{w_k} to 0;
  for each $F_i \in F (1 \le i \le n)$ **do**
    if F_i contains w_k **then**
      Set $v_{w_k}[i] = 1$;
    end if
  end for
end for
Set $V = \{v_{w_1}, v_{w_2}, ..., v_{w_m}\}$;
Randomly choose $x \in Z_q^*$, and compute $y = g^x$;
return (C, W, V, x, y);

Algorithm 2 IndexGen

Input: The secret key x, the keyword set W, the index vector set V.

Output: The secure index I.

1: **for** each $w_k \in W (1 \le k \le m)$ **do**
2: Extract v_{w_k} from V;
3: Compute $\pi(w_k)$;
4: Compute $ev_{\pi(w_k)} = v_{w_k} \oplus f(\pi(w_k))$;
5: Create an empty set $S_{w_k} = \emptyset$;
6: **for** each $i \in [1, n]$ **do**
7: **if** $v_{w_k}[i] == 1$ **then**
8: Add i to set S_{w_k};
9: **end if**
10: **end for**
11: **for** each $j \in [1, s]$ **do**
12: Compute:

$$\Omega_{w_k,j} = [(\prod_{i \in S_{w_k}} H_1(ID_i||j)^{-1}) \cdot H_3(j) \cdot H_2(\pi(w_k)||j)]^x$$

13: **end for**
14: Set $\Omega_{\pi(w_k)} = \{\Omega_{w_k,1}, \Omega_{w_k,2}, ..., \Omega_{w_k,s}\}$;
15: **end for**
16: **return** $I = \{\pi(w_k), ev_{\pi(w_k)}, \Omega_{\pi(w_k)}\}_{k=1,2,...,m}$;

VIII. RESULTS ANALYSIS

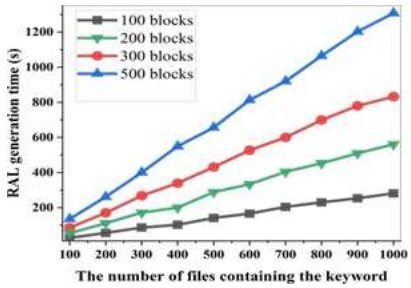


Fig. 1: The RAL generation time

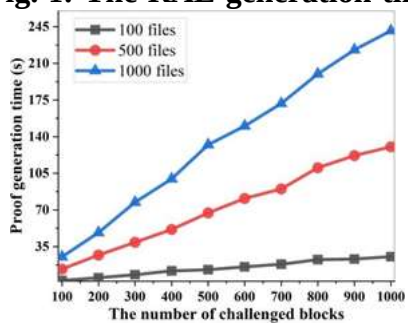


Fig. 2: The proof generation time

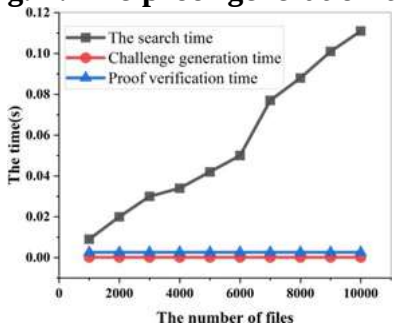


Fig. 3: The computation overhead comparison

IX. CONCLUSION

In this paper, we propose an efficient, secure and privacy preserving mobile cloud storage (MCS). The proposed scheme can protect data and access pattern simultaneously. Compared with existing schemes, our scheme has smaller item size, lightweight client-side computation and constant communication overhead. We also take temporal locality into consideration to further improve the efficiency of the scheme. By combining additional method, our scheme can be verifiable to resist malicious cloud. As a building block of the proposed MCS scheme, we also present an oblivious selection and update protocol, in which a client can obliviously select and update one of its encrypted data items outsourced in the cloud with a small vector. Due to small client computation and communication, we believe this protocol may be of independent interest for other secure multi-party computation application scenarios. The security and privacy proofs and analyses show that our scheme achieves data confidentiality and sufficient privacy preservation level. Finally, we compare our scheme with other two oblivious storage schemes and fully estimate our construction in a simulation environment. The results indicate that our scheme is significantly efficient and has good performances.

X. REFERENCES

[1] M. S. Islam, M. Kuzu, and M. Kantarcioglu, "Access pattern disclosure on searchable encryption: Ramification, attack and mitigation," in 19th Annual Network and Distributed System Security Symposium, NDSS 2012, San Diego, California, USA, February 5-8, 2012, 2012.

[Online].
Available:https://www.ndss-symposium.org/ndss2012/access-pattern-disclosure-searchable-encryption-ramification-attack-and-mitigation

[2] J. Kilian, "Founding cryptography on oblivious transfer," in Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA, 1988, pp. 20–31.[Online].
Available: https://doi.org/10.1145/62212.62215

[3] D. Boneh, D. Mazieres, and R. A. Popa, "Remote oblivious storage: Making oblivious ram practical," pp. 1–18, 2011.

[4] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," J.
ACM, vol. 43, no. 3, pp. 431–473, 1996. [Online]. Available:
http://doi.acm.org/10.1145/
233551.233553

[5] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorized private searches on public key encrypted data," in Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings, 2009, pp. 196–214. [Online]. Available: https://doi.org/10.1007/978-3-642- 00468-1 12

[6] T. Hoang, A. A. Yavuz, F. B. Durak, and J. Guajardo, "Oblivious dynamic searchable encryption via distributed PIR and ORAM," IACR Cryptology ePrint Archive, vol. 2017, p. 1158, 2017. [Online].
Available:http://eprint.iacr.org/2017/1158

[7] S. Garg, P. Mohassel, and C. Papamanthou, "TWORAM: efficient oblivious RAM in two rounds with applications to searchable encryption," in Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III, 2016, pp. 563–592. [Online]. Available: https://doi.org/10.1007/978-3-662- 53015-3

[8] E. Blass, T. Mayberry, G. Noubir, and K. Onarlioglu, "Toward robust hidden volumes usingwrite-only oblivious RAM," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014, 2014, pp. 203–214. [Online]. Available:http://doi.acm.org/10.1145/2660267.2660313

[9] D. S. Roche, A. J. Aviv, S. G. Choi, and T. Mayberry, "Deterministic, stash-free write-only ORAM," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017, 2017, pp.
507–521. [Online].
Available:http://doi.acm.org/10.1145/3133956.3134051

[10] E. Stefanov and E. Shi, "Oblivistore: High performance oblivious cloud storage," in 2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19-22, 2013, 2013,pp. 253–267. [Online]

Available: https://doi.org/10.1109/SP.2013.25

[11] D. Cash, A. K¨upc¸ ¨ u, and D. Wichs, "Dynamic proofs of retrievability via oblivious RAM," in Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, 2013, pp. 279–295. [Online]. Available: https://doi.org/10.1007/978-3-642-38348-9 17

[12] E. Stefanov and E. Shi, "Multi-cloud oblivious storage," in 2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013, 2013, pp. 247–258. [Online]. Available: http://doi.acm.org/10.1145/2508859.2516673

[13] B. Carbunar and R. Sion, "Write-once read-many obliviousRAM," IEEE Trans. Information Forensics and Security, vol. 6, no. 4, pp. 1394–1403, 2011.

[14] X. S.Wang, Y. Huang, T. H. Chan, A. Shelat,and E. Shi, "SCORAM: oblivious RAM for securecomputation," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014, 2014, pp. 191–202. [Online].

Available:https://doi.org/10.1145/2660267.2660365

[15] E. Boyle, K. Chung, and R. Pass, "Large-scale secure computation: Multi-party computation for (parallel) RAM programs," in Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II, 2015, pp.742–762. [Online].

Available: https://doi.org/10.1007/978-3-662-48000-7 36

[16] C. Gentry, K. A. Goldman, S. Halevi, C. S. Jutla, M. Raykova, and D. Wichs, "Optimizing ORAM and using it efficiently for secure computation," in Privacy Enhancing Technologies - 13th International Symposium, PETS 2013, Bloomington, IN, USA, July 10-12, 2013. Proceedings, 2013, pp. 1–18. [Online].

Available:https://doi.org/10.1007/978-3-642-39077-7 1

[17] S. Lu and R. Ostrovsky, "Distributed oblivious RAM for secure two-party computation," in Theory of Cryptography - 10th Theory of Cryptography Conference, TCC 2013, Tokyo, Japan, March 3-6, 2013. Proceedings, 2013, pp. 377–396. [Online]. Available: https://doi.org/10.1007/978-3-642- 36594-2 22

[18] S. Zahur, X. Wang, M. Raykova, A. Gasc´on, J. Doerner, D. Evans, and J. Katz, "Revisiting squareroot ORAM: efficient random access in multi-party computation," in IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, May 22-26, 2016, 2016, pp. 218–234. [Online].

Available: https://doi.org/10.1109/SP.2016.21

[19] D. Apon, J. Katz, E. Shi, and A. Thiruvengadam, "Verifiable oblivious storage,"

in Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26- 28, 2014. Proceedings, 2014, pp. 131–148. [Online]. Available:https://doi.org/10.1007/978-3-642-54631-0 8

[20] S. Devadas, M. van Dijk, C. W. Fletcher, L.Ren, E. Shi, and D. Wichs, "Onion ORAM: Aconstant bandwidth blowup oblivious RAM," inTheory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January10-13, 2016, Proceedings, Part II, 2016, pp. 145–174. [Online]. Available:https://doi.org/10.1007/978-3-662-49099-0 6

[21] A. Chakraborti, A. J. Aviv, S. G. Choi, T. Mayberry, D. S. Roche, and R. Sion, "roram: Efficient range ORAM with o(log2 N) locality," in 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019, 2019. [Online]. Available: https://www.ndss- symposium.org/ ndss-paper/roram-efficient-range- oram-with-olog2-n-locality/

[22] B. Pinkas and T. Reinman, "Oblivious RAMrevisited," in Advances in Cryptology - CRYPTO2010, 30th Annual Cryptology Conference, SantaBarbara, CA, USA, August 15- 19, 2010.Proceedings, 2010,pp. 502–519. [Online]. Available:https://doi.org/10.1007/978-3-642-14623-7 27

[23] I. Damg°ard, S. Meldgaard, and J. B. Nielsen,"Perfectly secure oblivious RAM without random oracles," in Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings, 2011, pp. 144–163. [Online]. Available: https://doi.org/10.1007/978-3-642-19571-6 10

[24] E. Shi, T. H. Chan, E. Stefanov, and M. Li, "Oblivious RAM with O((logN)3) worst-case cost," in Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011.Proceedings, 2011, pp. 197–214. [Online]. Available: https://doi.org/10.1007/978-3-642-25385-0 11

[25] E. Stefanov, E. Shi, and D. X. Song, "Towards practical oblivious RAM," in 19th Annual Networkand Distributed System Security Symposium, NDSS 2012, San Diego, California, USA, February 5-8, 2012, 2012. [Online]. Available: https://www.ndss-symposium. org/ndss2012/towards-practical-oblivious-ram.

AUTHOR PROFILE:

[1] Mr. K. Jaya Krishna, currently working as an Associate Professor in the Department of Master of Computer Applications, QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He did his MCA from Anna University, Chennai, M.Tech (CSE) from JNTUK, Kakinada. He published more than 10 research papers in reputed peer reviewed Scopus indexedjournals. He also attended and presented

research papers in different national and international journals and the proceedings were indexed IEEE. His area of interest is Machine Learning, Artificial intelligence, Cloud Computing and Programming Languages.

[2] [Mr. Yeruva Venkata Reddy, currently pursuing Master of Computer Applications at QIS College of Engineering and Technology (Autonomous), Ongole, Andhra Pradesh. He Completed B.Sc. in Computer Science from Kartikeya Degree College, Ongole, Andhra Pradesh. His areas of interests are Cloud Computing & Machine learning.