International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

An Exploration on Privacy Concerned Secured Data Sharing Techniques in Cloud

P Raja Sekhar Reddy, K Ravindranadh

Abstract: ***Cloud service is the most popular environment utilized by millions of users for different kind of service utilization. Cloud services needs to be provided with the concern of satisfying user requirements to increase their popularity level. The main issues associated with cloud service handling are maintaining integrity of data, user management, secured data transmission and so on. These issues are addressed by various authors by introducing the different methodologies. In this analysis work, discussion about those research techniques has been given with the detailed explanation. This paper provides the overview about the different research techniques whose main goal is to achieve the increase the data integrity level of the shared data. This paper also provides the discussion about various dynamic grouping techniques which tends to provide more flexible access to the user revocation. Different research techniques proposed by various authors has been described and compared their performance in terms of merits and demerits each research technique. The overall evaluation of the research technique is done based on numerical outcome present in each research technique and best research technique has been found***

Keywords: ***Cloud services, data integrity, user privacy requirements, authentication, user revocation, dynamic grouping***

I. INTRODUCTION

Cloud computing is the most prominent administrations used by a huge number of clients. Cloud computing offers different administrations to the clients dependent on their necessity in the virtualized group [1]. One of the most significant administrations gave the cloud asset suppliers is capacity administration [2]. Different businesses and association endeavors use the capacity administration given by the cloud model [3]. Here clients pay for the measure of capacity they used once. At the time of storing the personal details in the third party cloud providers, there is a chance of occurrence of many issues [4]. One of the most found threat is data integrity and privacy issues. Malicious users in the cloud environment might attempt to steal or corrupt the information that is stored in the third party service providers [5].

Data integrity is the main property of data storage which should be high [6]. Data integrity defines maintaining the fresh copy of data when it is accessed by multiple users. The users should be provided with the most recently updated copy of data when it is shared among multiple users present in multiple servers [7]. Achieving high level of data integrity is most difficult task which needs to be done with more concern to improve the user satisfaction level. This can be achieved in various ways. One of the most popular way is signature based sharing scheme where the each user who access the data copy need to generate the signature from which user who accessed data copy lastly can be predicted [8]. From this most recent copy of data can be shared with the other users.

Another important issue that occurs in the cloud storage service is the user privacy [9]. As millions of users attempts to utilize the cloud storage for storing their contents, privacy issues also increased considerably.

Users are not ready to share their identity information to the other third party service providers because of their privacy concern [10]. There is various research techniques has been introduced earlier for the implementation of privacy requirements of the users.

Privacy implementation can be attained by using the encryption techniques where instead of gathering the identity information, some random information will be gathered from the cloud users [11]. By using this information cloud stored data contents will be encrypted and will be shared with other users [12]. Thus the privacy requirements of the cloud users can be ensured.

In case of finding the malicious activities inside the cloud environment, malicious users need to be eliminated from the network to avoid the unwanted data corruption or stealing [13]. User revocation is the process of eliminating the unwanted users from the cloud network to protect the data from the malicious providers. This can be achieved by introducing the various methodologies that can revoke the users from the environment efficiently.

In this analysis work, discussion of different methodologies is given that ensure the proper and efficient functioning of the cloud environment. This paper provides overview of various data integrity techniques, privacy implementation techniques and user revocation techniques. The detailed description of these techniques is given in this work with their working procedure and the functionality. The comparison evaluation of these research techniques are given based on different merits and demerits to prove the performance improvement.

In this section general overview of cloud environment and main issues involved in the cloud environment is given. In section 2, different data integrity maintenance techniques have been given with their detailed working procedure. This section also provides the comparison evaluation of the various research techniques based on their merits and demerits.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
P Raja Sekhar Reddy *, Research Scholar., KLEF, Vaddeswaram, AP, India. Email: prreddy.cvsr@gmail.com
K Ravindranadh , CSE, KLEF, Vaddeswaram, AP, India. Email: ravindra_ist@kluniversity.in

Likewise in section 3 and 4, discussion of different dynamic grouping techniques and privacy implementation techniques are provide along with comparison of methodologies based on merits and demerits. In section 5, comparison of different research techniques based on numerical outcome is given. Finally in section 6, conclusion of these analysis results is given.

II. DISCUSSION OF DIFFERENT DATA INTEGRITY MAINTENANCE TECHNIQUES

Hao et al [14] proposed new protocol which tends to ensure the data integrity level. The objective of this paper is to ensure the privacy level of the cloud users by adapting the public verification. Privacy guidance of the cloud users are ensured by protecting the private information of the cloud users without leakage. The overall implementation of this work ensures the increased security level with guaranteed privacy preservation. This research technique guarantees the data dynamic verification by improving the various attribute implementation.

Wang et al [15] introduced ring based privacy auditing protocol for ensuring the secured information sharing in the cloud. This method will collect the verification information from the users based on which data auditing will be performed. The objective of this research method is to ensure the privacy of the cloud users with the help of third party service providers. This research work also guarantees the data integrity level of the cloud servers by verifying the cloud user information. The comparison evaluation of the research work proved proposed research work tends to provide the effective and efficient cloud storage services with assured privacy requirements.

Wang et al [16] presented the new open confirmation technique for guaranteeing the information trustworthiness level. This strategy adjusts the multi mark plot for guaranteeing the information respectability level. The primary objective of this examination work is to guarantee the information honesty level with decreased confirmation time and capacity overhead. The general assessment of the exploration work is done in the untrusted cloud condition and guaranteed the information uprightness level for the information gathered from the numerous proprietors. The usage of this examination work guarantees the better information trustworthiness level with ensured security safeguarding.

Wang et al [17] introduced secured model for the secure and reliable data sharing by introducing the intermediary information sharing mechanism. The proposed research work is mainly based on the key sharing procedures based on which bilinear pairing will be performed. The performance assessment of this work ensured computational effective of entire research work in terms of increased security level.

Yu et al [18] presented the novel convention which depends on personality based cryptographic instrument. The primary objective of this exploration work is to guarantee the expanded information respectability level for the cloud put away information substance. This exploration work likewise ensures the assurance from protection data spillage. This is finished by utilizing RDIC convention which will in general guarantee the expanded security level with the assistance of outsider verifier. The proposed technique ensures the expanded information respectability level by adjusting nonexclusive gathering model with the security from the noxious specialist co-ops.

Shao et al [19] proposed dynamic information honesty evaluating strategy for guaranteeing the security level of the cloud condition. This is finished by executing the technique in particular progressive different branches tree based information validation strategy. This strategy guarantees the dynamic information updation process with expanded security insurance from the noxious clients. This technique likewise adjusts the advanced mark plot for guaranteeing the security assurance of the numerous clients. The exhibition examination of the exploration work will in general demonstrate expanded security level with the assurance from the different assaults, for example, fabrication assaults.

Shen et al [20] proposed remote based information trustworthiness evaluating technique for the productive sharing help for the cloud clients. This technique empowers clients to proficiently share the touchy data to the cloud clients dependent on mark created on numerous information squares. This examination method will in general guarantee the better security protection with ensured character based cryptography strategy. This proposed strategy will purify the delicate data which will be escaped other cloud clients and the vindictive specialist organizations. The security examination of the exploration work demonstrated that the proposed strategy will in general have preferred execution over the current systems.

Arshad et al [21] endeavored to guarantee the expanded information uprightness level for the chart databases. The fundamental objective of this exploration work is to guarantee the adaptable and dependable information honesty checking for the diagram databases which is progressively perplexing to deal with. This examination work underpins the dynamic expansion and end of vertices into the condition This exploration strategy bolsters the two party information sharing and the outsider information partaking in the cloud condition for the proficient stockpiling and upkeep. The trial result of the exploration procedures will in general give the better result as far as quicker correspondence strings.

Lu et al [22] endeavored to play out the information uprightness checking with decreased expense of procedure. This is finished by presenting the strategy to be specific Merkel Hash Tree (MHT) which endeavors to guarantee the information trustworthiness checking in the solid way. The proposed research procedure will in general have better information respectability checking support by presenting the strategy to be specific RDIC conspire. The fundamental objective of this exploration work is to guarantee the information respectability level for the huge diagram information. The general assessment of this model demonstrated that the proposed procedure guarantees better information trustworthiness under arbitrary prophet model.

Liu et al [23] proposed the system to be specific LiveForen. The fundamental objective of this exploration work is to guarantee the expanded information uprightness level for the powerfully gathered criminological information from the different web sources. This is achieved by presenting the two web source conventions to be specific confided in stage module and the characteristic based encryption.

The general assessment of the exploration work guarantees the proposed research procedure ensures the better correspondence execution with expanded security level by watermarking the mystery data with the info pictures.

Table 1. Comparison of Data integrity techniques

S.No	Author	Method	Merits	Demerits
1	Hao et al (2011)	Remote data integrity checking	Great improvement as far as correspondence cost, calculation cost and capacity cost Better privacy preservation	Increased volume of data will lead to increased data communication and computation cost
2	Wang et al (2014)	Oruta	Increased effectiveness in public auditing Improved efficiency Ensured privacy preservation	Increased computation overhead
3	Wang et al (2014)	public verification method	Increased data integrity level Improved multi signature authentication Increased security level	More computation overhead
4	Wang et al (2016)	Identity-based proxy-encryption method	Increased data integrity level Increased privacy level More security	Computational cost is high
5	Yu et al (2016)	Identity based cryptographic mechanism	Better privacy protection than the existing methods Better resistant from forgery attacks Increased security level	Increased data communication cost
6	Shao et al (2018)	Dynamic data auditing method	Better resistance forgery attacks Better support to dynamic updating process Increased performance efficiency	Lacks in privacy protection with the presence of multiple data owners
7	Shen et al (2018)	Remote based data integrity auditing method	Proposed method is more secured It provides more efficient outcome More reliable cloud storage	Increased storage cost
8	Arshad et al (2018)	Scalable data integrity verification	Faster communication Ensured data integrity level Optimal maintenance of graph databases	Reduced privacy Computation hard to ensure the security level
9	Lu et al [2019]	Merkel Hash Tree algorithm	Increased security level for the big graph data Better public verification scheme Better privacy preservation in big graph data	User revocation is not supported
10	Liu et al (2019)	LiveForen	Increased data integrity level Better scalability support Reduced communication overhead	Cannot tolerate big data

III. DISCUSSION OF DIFFERENT PRIVACY IMPLEMENTATION TECHNIQUES

Zhang et al [24] presented protection spillage upper bound imperative based methodology for guaranteeing the security prerequisites for the cloud clients. This research work ensures the cost effective computing outcome. The primary objective of this examination work is to execute the financially savvy protection saving strategy for the middle of the road informational collections that are store in the cloud condition. The proposed research strategy will in general counteract the spillage of security prerequisites of information substance that are put away in the distributed storage. The general assessment of the examination procedures will in general improve the better execution with decreased correspondence cost and expanded security protection.

Rahulamathavan et al [25] introduced the multi class support vector machine for the better privacy preservation for the cloud stored data contents. The objective of this paper is to ensure the privacy level with reduced storage cost. This is done by outsourcing the data classification process to the third part service providers. In third party service provider's better classification outcome is ensured by adapting the multi class support vector machine. This research method tends to ensure the better privacy preservation outcome with increased security level.

Cao et al [26] introduced the multi keyword ranked search scheme with the concern of the privacy preservation. The main goal of this research work is to ensure the security level with guaranteed attribute matching. The research work also supports the reliable key word based search retrieval outcome by retrieving the most top ranked documents to the cloud users based on their submitted keywords. Similar retrieval of documents are ensured by adapting the inner product similarity computation techniques which tends to ensure the most optimal and reliable outcome.

Zhang et al [27] built up a novel time-arrangement example based commotion age methodology for security assurance on cloud. To start with, we dissect this security hazard and present a novel bunch based calculation to create time interims powerfully. At that point, in light of these time interims, we research relating likelihood vacillations and propose a novel time-arrangement example based anticipating calculation. Ultimately, in light of the estimating calculation, our novel commotion age procedure can be introduced to withstand the likelihood vacillation security chance. The reproduction assessment shows that our methodology can essentially improve the adequacy of such cloud security assurance to withstand the likelihood variance protection hazard.

Zhang et al [28] attempted to preserve the users privacy requirements of users for the big data. This is done by introducing the method namely proximity aware local recoding anonymisation technique. This research techniques tends to ensure the better privacy preservation for the big data. This is done by introducing the methods namely two clustering techniques namely k means clustering method and the agglomerative clustering technique. This work adapted the map reduce framework to support the increased scalability process. The performance evaluation of the research work tends to provide the better outcome with better scalability support and the time efficiency.

Liu et al [29] introduced the privacy aware authentication protocol for ensuring the privacy requirements of cloud users. In this work, authorities of multiple users are preserved by adapting the multiple users sharing request. This is done by adapting the attribute based encryption method where the attribute information of multiple users will be collected based on which authentication will be performed. The overall evaluation of the research technique tends to prove that the shared authority privacy preservation can be enhanced and the security level is enhanced by adapting the proxy reencryption technique.

Zhang et al [30] considered the issue of protection safeguarding set-esteemed information distributing. Existing information protections saving procedures are not pertinent in numerous genuine scenes. Propelled by this perception, creators displayed a suite of new procedures that make security mindful set-esteemed information distributing doable on crossover cloud. On information distributing stage, proposed an information segment procedure, named broadened semi identifier-parceling, which disassociates record terms that partake in distinguishing blends.

Islam et al [31] endeavored to execute the security and protection prerequisites of the cloud sending models. This examination work investigated the significant points of view of the security and protection necessities of the distinctive cloud organization models. The work presents assertion as verification for satisfying the security and insurance requirements to the extent perfection and reportable of security scene through survey.

Shen et al [32] introduced the security mechanism namely connor with the goal of ensuring the privacy preservation. The objective of this paper is to introduce the computationally efficient and encrypted mechanism to ensure the computationally efficient outcome. This research method attempts to encrypt the graphs to protect the sensitive information in the efficient way. The performance evaluation proved that the proposed research method tends to provide the better outcome in terms of increased performance evaluation.

Cheng et al [33] proposed accountable privacy preserving method for the ensuring the security methods and the privacy requirements. This is done by considering the various privacy requirements that are specified by the customer. The proposed research technique ensures the security level by adapting the identity based encryption procedure. The research method focuses on the two different attacks that are mainly happening on the cloud. The overall evaluation of the research method is to implement the research technique that can ensure the optimal and efficient security implementation.

Table 2. Comparison of privacy implementation technique

S.No	Author	Method	Merits	Demerits
1	Zhang et al (2012)	Privacy leakage upper bound constraint based approach	Reduced communication cost Better data integrity support Better prevention of privacy requirements leakage	More storage cost
2	Rahulamathavan et al (2013)	multi class support vector machine	Increased security level Better privacy maintenance Reliable handling of large volume of data	Increased computation overhead
3	Cao et al (2013)	multi keyword ranked search scheme	Ensure the privacy preservation Ensured top k similar document retrieval Reduced communication time	With the presence of malicious nodes integrity checking is difficult
4	Zhang et al (2014)	Time series pattern based noise generation model	Increased efficiency Improved privacy preservation Better fluctuation probability risk	Increased noise level would lead to reduced performance

5	Zhang et al (2014)	proximity aware local recoding anonymisation technique	Better time efficiency Increased scalability Better anonymisation support by preserving the privacy requirements	Increased data volume might degrade the performance
6	Liu et al (2014)	shared authority based privacy preserving authentication protocol	Increased security level Enhanced privacy preservation Better support to the data sharing to the multiple users	More computation overhead
7	Zhang et al (2015)	Privacy-aware set-valued data publishing method	Increased scalability Enhanced privacy preservation of cloud user identity Better security level Reduced information loss	Querying is difficult Increased communication cost
8	Islam et al (2015)	Analysis of security requirements	Provides the better security implementation techniques Increased privacy requirement level	Need more focus towards the privacy requirements
9	Shen et al (2017)	Connor	Improved efficiency Increased security level Better privacy protection	It doesn't support the dynamic index updates
10	Cheng et al (2018)	accountable privacy preserving method	Guaranteed security preservation Ensured privacy preservation Better accountability	User privacy preservation is more difficult

IV. DISCUSSION OF DIFFERENT DYNAMIC GROUPING TECHNIQUES

Zhu et al [34] introduced secured data sharing platform to support the dynamic cloud. This is done by circulating the key through out the cloud in the secured way based on which secured data sharing will be performed. This research work also supports fine grained access control to support the efficient and reliable data sharing with supported flexibility and scalability.

Chen et al [35] introduced the clustering mechanism for the grouping the scientific workflows gathered from the web. The main goal of this research work is to cluster the input workflows with the concern of fault tolerance. This research work ensures the fault free clustering outcome with the presence of various objectives such as fault tolerance attributes. This research work also supports the dynamic clustering outcome with the concern of reducing the makespan time. This research work also ensures the granularity free clustering outcome in the dynamic way.

Lingwei et al [36] presented the figure content arrangement and characteristic based encryption method for guaranteeing the security and protection necessities of the cloud clients.

This exploration strategy fundamentally centers around the malignant client renouncement with the worry of ensured information secrecy. The general assessment of the examination work ensures the fine grained information access control method with guaranteed client disavowal result. This examination strategy likewise underpins the expanded adaptability result with ensured client access control execution. This exploration technique ensures the information secrecy of cloud put away information.

Raghavendra et al [37] presented the verified multi proprietor information sharing plan for the verified and security safeguarded information sharing result. This examination work ensures the verified information sharing result in the dynamic route by adjusting the RSA Chinese leftover portion hypothesis which guarantees the expanded security level. The security and protection necessities of the examination methods are guaranteed by presenting the key administration technique with the objective of diminishing the capacity cost and calculation overhead.

Xu et al [38] proposed the verified fine grained access control conspire for guaranteeing the security level and actualizing the protection necessities in the proficient manner. The general assessment of the examination work is finished with the worry of expanding the security level and improving the protection necessities.

This exploration procedure ensures the better client renouncement result by presenting the revocable property based encryption strategy. The reenactment results demonstrated that the proposed research system ensures the effective and adaptable result in the proficient manner.

Yuan et al [39] introduced the deduplication procedure for the enhanced cloud storage performance by reducing the computation overhead. The proposed method supports the scalable and flexible data storage by supporting the unapproved clients also into the environment. Here security is enhanced by performing the authentication process.

Cui et al [40] focused on sharing the data with the multiple users from the different domains. This is done by introducing the attribute based encryption which enhances the network performance by extracting the different structural properties. The overall evaluation of the research work is implemented in the cloud simualitn and client access control is performed efficiently.

Luo et al [41] proposed a novel open inspecting plan for the honesty of imparted information to proficient conspiracy safe client renouncement. Furthermore, we stretch out the proposed plan to help safely signature and confirmation re-appropriating, which permit more productivity for gathering clients and the examiner. The numerical examinations and exploratory outcomes exhibit that our plan is provably secure and very effective, the re-appropriating calculations make the marks age and confirmation process increasingly productive and moderate for cell phones.

He et al [42] presented the light weight characteristic based encryption strategy for guaranteeing the security level and the protection usage. This is accomplished by presenting the different research procedures which ensures the security level. This is accomplished by presenting the confirmation and encryption method dependent on which security can be guaranteed. The fundamental objective of this exploration work is to guarantee the ideal and solid result as far as better fine grained access control result. This examination strategy additionally ensures the better result with diminished computational overhead.

Peng et al [43]introduced replication aware data possession method which can support efficient and dynamic data storage and sharing process. The overall evaluation of the research work is implemented and it is confirmed that the proposed research technique enhances the data security along with increased data scalability and flexibility.

Table 3. Comparison of dynamic grouping techniques

S.No	Author	Method	Merits	Demerits
1	Zhu et al (2015)	Secured data sharing scheme	Better user revocation Ensured privacy preservation Increased security level	More computation overhead
2	Chen et al (2015)	Fault tolerant clustering	Reduced makespan value Supports dynamic clustering outcome Reduced granularity	Unexpected situation might lead to reduced system performance
3	Lingwei et al (2015)	cipher text policy and attribute based encryption technique	Better scalability Better fine grained access control Increased security level	Failed to provide resistance to the malicious attacks
4	Raghavendra et al (2016)	secured multi owner data sharing scheme	Reduced storage cost Reduced computation overhead Optimal utilization of the storage space	Computationally slow in retrieval outcome
5	Xu et al (2018)	secured fine grained access control scheme	Supports scalability Better dynamic support Efficient user revocation outcome	Forage attacks cannot be predicted

6	Yuan et al (2018)	Scalable data deduplication method	Reduced communication overhead Efficient encryption outcome Increased scalability Better dynamic user management	Increased storage cost
7	Cui et al (2018)	Attribute based encryption	Increased collusion resistance Better semantic security implementation Increased security level	Inefficient user revocation support
8	Luo et al (2018)	Public auditing scheme	More efficient More affordable Increased scalability Better user revocation outcome	Increased computation overhead
9	He et al (2018)	light weight attribute based encryption method	Reduced computational overhead Increased security level Ensured privacy preservation	User revocation is not performed efficiently
10	Peng et al (2019)	identity-based RDIC scheme	Computationally efficient Better privacy preservation Optimal storage maintenance	Inefficient performance with the presence of large scale applications

V. CONCLUSION

This paper provides the overview about the different research techniques whose main goal is to achieve the increase the data integrity level of the shared data. This paper also provides the discussion about various dynamic grouping techniques which tends to provide more flexible access to the user revocation. Different research techniques proposed by various authors has been described and compared their performance in terms of merits and demerits each research technique. The overall evaluation of the research technique is done based on numerical outcome present in each research technique and best research technique has been found.

REFERENCE

1. Rittinghouse, J. W., & Ransome, J. F. (2017). Cloud computing: implementation, management, and security. CRC press.
2. Ren, Y. J., Shen, J., Wang, J., Han, J., & Lee, S. Y. (2015). Mutual verifiable provable data auditing in public cloud storage. *網際網路技術學刊*, *16*(2), 317-323.
3. Yang, H. L., & Lin, S. L. (2015). User continuance intention to use cloud storage service. *Computers in Human Behavior*, *52*, 219-232.
4. Mazrekaj, A., Shabani, I., & Sejdiu, B. (2016). Pricing schemes in cloud computing: an overview. *International Journal of Advanced Computer Science and Applications*, *7*(2), 80-86.
5. Aldossary, S., & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *International Journal of Advanced Computer Science and Applications*, *7*(4), 485-498.
6. Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., & Min, G. (2016). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. *IEEE Transactions on Information Forensics and Security*, *12*(4), 767-778.
7. Tan, S., Jia, Y., & Han, W. H. (2015). Research and development of provable data integrity in cloud storage. *Chinese Journal of Computers*, *38*(1), 164-177.
8. Zhu, H., Tan, Y. A., Zhang, X., Zhu, L., Zhang, C., & Zheng, J. (2017). A round-optimal lattice-based blind signature scheme for cloud services. *Future Generation Computer Systems*, *73*, 106-114.
9. Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., & Min, G. (2016). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. *IEEE Transactions on Information Forensics and Security*, *12*(4), 767-778.
10. Song, W., Wang, B., Wang, Q., Peng, Z., Lou, W., & Cui, Y. (2017). A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications. *Journal of Parallel and Distributed Computing*, *99*, 14-27.

11. Xia, Z., Wang, X., Zhang, L., Qin, Z., Sun, X., & Ren, K. (2016). A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. *IEEE Transactions on Information Forensics and Security*, *11*(11), 2594-2608.
12. Salam, M. I., Yau, W. C., Chin, J. J., Heng, S. H., Ling, H. C., Phan, R. C., ... & Yap, W. S. (2015). Implementation of searchable symmetric encryption for privacy-preserving keyword search on cloud storage. *Human-centric Computing and Information Sciences*, *5*(1), 19.
13. Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers & Security*, *74*, 340-354.
14. Hao, Z., Zhong, S., & Yu, N. (2011). A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability. *IEEE transactions on Knowledge and Data Engineering*, *23*(9), 1432-1437
15. Wang, B., Li, B., & Li, H. (2014). Oruta: Privacy-preserving public auditing for shared data in the cloud. *IEEE transactions on cloud computing*, *2*(1), 43-56.
16. Wang, B., Li, H., Liu, X., Li, F., & Li, X. (2014). Efficient public verification on the integrity of multi-owner data in the cloud. *Journal of Communications and Networks*, *16*(6), 592-599.
17. Wang, H., He, D., & Tang, S. (2016). Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud. *IEEE Transactions on Information Forensics and Security*, *11*(6), 1165-1176.
18. Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., & Min, G. (2016). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. *IEEE Transactions on Information Forensics and Security*, *12*(4), 767-778.
19. Shao, B., Bian, G., Wang, Y., Su, S., & Guo, C. (2018). Dynamic Data Integrity Auditing Method Supporting Privacy Protection in Vehicular Cloud Environment. *IEEE Access*, *6*, 43785-43797.
20. Shen, W., Qin, J., Yu, J., Hao, R., & Hu, J. (2018). Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage. *IEEE Transactions on Information Forensics and Security*, *14*(2), 331-346.
21. Arshad, M. U., Kundu, A., Bertino, E., Ghafoor, A., & Kundu, C. (2018). Efficient and scalable integrity verification of data and query results for graph databases. *IEEE Transactions on Knowledge and Data Engineering*, *30*(5), 866-879.
22. Lu, Y., & Hu, F. (2019). Secure Dynamic Big Graph Data: Scalable, Low-Cost Remote Data Integrity Checking. *IEEE Access*, *7*, 12888-12900.
23. Liu, A., Fu, H., Hong, Y., Liu, J., & Li, Y. (2019). LiveForen: Ensuring Live Forensic Integrity in the Cloud. *IEEE Transactions on Information Forensics and Security*.
24. Zhang, X., Liu, C., Nepal, S., Pandey, S., & aayvusdcf u,.\'Chen, J. (2012). A privacy leakage upper bound constraint-based approach for cost-effective privacy preserving of intermediate data sets in cloud. *IEEE Transactions on Parallel and Distributed Systems*, *24*(6), 1192-1202.
25. Rahulamathavan, Y., Phan, R. C. W., Veluru, S., Cumanan, K., & Rajarajan, M. (2013). Privacy-preserving multi-class support vector machine for outsourcing the data classification in cloud. *IEEE Transactions on Dependable and Secure Computing*, *11*(5), 467-479.
26. Cao, N., Wang, C., Li, M., Ren, K., & Lou, W. (2013). Privacy-preserving multi-keyword ranked search over encrypted cloud data. *IEEE Transactions on parallel and distributed systems*, *25*(1), 222-233.
27. Zhang, G., Liu, X., & Yang, Y. (2014). Time-series pattern based effective noise generation for privacy protection on cloud. *IEEE Transactions on Computers*, *64*(5), 1456-1469.
28. Zhang, X., Dou, W., Pei, J., Nepal, S., Yang, C., Liu, C., & Chen, J. (2014). Proximity-aware local-recoding anonymization with mapreduce for scalable big data privacy preservation in cloud. *IEEE transactions on computers*, *64*(8), 2293-2307
29. Liu, H., Ning, H., Xiong, Q., & Yang, L. T. (2014). Shared authority based privacy-preserving authentication protocol in cloud computing. *IEEE Transactions on parallel and distributed systems*, *26*(1), 241-251.
30. Zhang, H., Zhou, Z., Ye, L., & Du, X. (2015). Towards privacy preserving publishing of set-valued data on hybrid cloud. *IEEE Transactions on cloud computing*, *6*(2), 316-329.
31. Islam, S., Ouedraogo, M., Kalloniatis, C., Mouratidis, H., & Gritzalis, S. (2015). Assurance of security and privacy requirements for cloud deployment models. *IEEE Transactions on Cloud Computing*, *6*(2), 387-400.
32. Shen, M., Ma, B., Zhu, L., Mijumbi, R., Du, X., & Hu, J. (2017). Cloud-based approximate constrained shortest distance queries over encrypted graphs with privacy protection. *IEEE Transactions on Information Forensics and Security*, *13*(4), 940-953.
33. Cheng, H., Rong, C., Qian, M., & Wang, W. (2018). Accountable Privacy-Preserving Mechanism for Cloud Computing Based on Identity-Based Encryption. *IEEE Access*, *6*, 37869-37882.
34. Zhu, Z., & Jiang, R. (2015). A secure anti-collusion data sharing scheme for dynamic groups in the cloud. *IEEE Transactions on parallel and distributed systems*, *27*(1), 40-50.
35. Chen, W., da Silva, R. F., Deelman, E., & Fahringer, T. (2015). Dynamic and fault-tolerant clustering for scientific workflows. *IEEE Transactions on Cloud Computing*, *4*(1), 49-62.
36. Lingwei, S., Fang, Y., Ru, Z., & Xinxin, N. (2015). Method of secure, scalable, and fine-grained data access control with efficient revocation in untrusted cloud. *The Journal of China Universities of Posts and Telecommunications*, *22*(2), 38-43.
37. Raghavendra, S., Meghana, K., Doddabasappa, P. A., Geeta, C. M., Buyya, R., Venugopal, K. R., & Patnaik, L. M. (2016). Index generation and secure multi-user access control over an encrypted cloud data. *Procedia Computer Science*, *89*, 293-300
38. Xu, S., Yang, G., Mu, Y., & Deng, R. H. (2018). Secure fine-grained access control and data sharing for dynamic groups in the cloud. *IEEE Transactions on Information Forensics and Security*, *13*(8), 2101-2113.
39. Yuan, H., Chen, X., Jiang, T., Zhang, X., Yan, Z., & Xiang, Y. (2018). DedupDUM: Secure and scalable data deduplication with dynamic user management. *Information Sciences*, *456*, 159-173
40. Cui, J., Zhou, H., Zhong, H., & Xu, Y. (2018). AKSER: Attribute-based keyword search with efficient revocation in cloud computing. *Information Sciences*, *423*, 343-352.
41. Luo, Y., Xu, M., Huang, K., Wang, D., & Fu, S. (2018). Efficient auditing for shared data in the cloud with secure user revocation and computations outsourcing. *Computers & Security*, *73*, 492-506.
42. He, Q., Zhang, N., Wei, Y., & Zhang, Y. (2018). Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems. *Computer Networks*, *140*, 163-173.
43. Peng, S., Zhou, F., Li, J., Wang, Q., & Xu, Z. (2019). Efficient, dynamic and identity-based Remote Data Integrity Checking for multiple replicas. *Journal of Network and Computer Applications*, *134*, 72-88.

AUTHORS PROFILE

Mr. P.Raja sekhar Reddy Pursuing Ph.D in CSE at KL University, Vaddeswaram, AP, India and received M.Tech degree in Computer Science and Engineering at JNTU Hyderabad. His research area includes Cloud Computing and IoT. He has got twelve years of teaching experience. Currently working as Asst.Professor in Anurag Group of Institutions Hyderabad. He has published 10 papers in various national and International Journals .He attended 4 International Conferences, attended close to twenty workshops and got memberships from ISTE and IAEng.

K.Ravindranath received a Ph.D degree from Achrya Nagarjuna University in 2016. Currently, he is Associate Professor of Computer Science & Engineering at K L University, Vaddeswaram, AP, India. Prof. Ravindranath's research interests include Cloud, Mobile Clouds and Security. His work has appeared in over 24 publications. He is a member of ACM, Senior Life member in Computer Society of India.