iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4314

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: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Outsourcing Data based on Key Exchange and File Encryption with Integrity Check

Anusree M P[1], Sreekala R[2]
[1]*PG Scholar at Jawaharlal College of Engineering and Technology, Palakkad, India*
[2]*Assistant professor at Jawaharlal College of Engineering and Technology, Palakkad, India*

Abstract: ***Cloud computing is a developing innovation and it gives different services to clients. The most attractive service of cloud computing is Data outsourcing. By Data Outsourcing the data owners can have any size of data on the cloud server and clients can retrieve data from cloud server when required. Cloud storage system provides facilitative file storage and sharing services for distributed clients. To address controllable outsourcing, integrity and origin auditing concerns on outsourced files, proposes an Identity Based Data Outsourcing (IBDO) scheme outfitted with attractive highlights worthwhile over existing systems in securing outsourced data. First, IBDO scheme allows a user to authorize devoted intermediaries that means dedicated proxies to upload data to the cloud storage server on her behalf, e.g., an organization may approve a few workers (proxies) to transfer documents to the organization's cloud account in a controlled way. In IBDO framework, to designate outsourcing rights to a proxy, the administrator signs a committed warrant for the proxy. The warrant may indicate who can outsource which sort of documents during what time in the interest of the data owner. The proxies are authorized and identified with their recognizable identities, which takes out complicated certificate management in usual secure distributed computing systems. The key exchange between administrator and users are done by ECDH (Elliptical Curve Diffie Hellman) algorithm. Second, IBDO scheme facilitates comprehensive auditing, that is, IBDO scheme not just allows regular integrity auditing as in existing schemes for securing outsourced data, yet in addition permits to audit the information on data origin, type, and consistence of outsourced files. The security of the files are also ensured in this system by encrypting the files using AES (Advanced Encryption Standard) algorithm.***

Keywords: Cloud storage, Data outsourcing, Proof of storage, Remote integrity proof, Public auditing.

I. INTRODUCTION

Cloud computing has brought a lot of benefits to the computing world. It empowers to share computing resources without the requirement for interest in pay as you use form, so without capital investment individuals and organizations can utilize storage and other services provided by cloud. Virtualization is the basic concept behind cloud computing. It provides computing service and virtual storage to the cloud users. Availing resources is the key role of virtualization the resources include operating system, network, storage device and server, so that multiple users can use resources at the same time. Cloud storage can make data users store and access their files anytime, from anywhere and with any device [19]. The importance of cloud storage service is more and more highlighted with the development of cloud computing techniques and the exponential growth in data. Cloud storage allows data owners to move data from their local computing systems to the Cloud [24]. The main reason behind more and more data owners start choosing to host their data in the Cloud is because of cost effectiveness, which is particularly true for medium-sized and small businesses. Data owners can avoid the initial investment of expensive infrastructure setup, large equipment's, and daily maintenance cost by hosting their data in the Cloud. The data owners just need to pay the space they really utilize. Another reason is that data owners can rely on the Cloud to provide more reliable services, so that they can retrieve data from anyplace and whenever. Usually small-sized companies or Individuals do not have the resource to keep their servers as reliable as the Cloud does. People begin to use cloud storage services to keep their important files. And it has also become a trend that individuals and IT enterprises store their data to the cloud in a flexible on demand manner since it can reduce the burden for storage management and maintenances and costs on hardware and software, and provide convenient access to the outsourced data.

Cloud computing is broadly used by various organization for data outsourcing [16]. Without any geographical restriction end user cloud computing provides flexible and cost effective way to access outsourced data to in multiform. Numerous organizations outsource data storage to the cloud such that a member (owner) of an organization can easily share data with other members (users).Despite the fact that cloud storage provides great advantages and conveniences for the users, it faces numerous new security challenges [18] since the user no longer possesses their data locally. The storage facilities are under control of cloud service

providers and users are losing control over their data. The security challenges are firstly, data owners would worry their data could be misused or accessed by unauthorized users. Secondly, the data owners would worry their data could be lost in the Cloud. This is because data loss could happen in any infrastructure, even though cloud service providers give high degree of reliable measures. Sometimes, the cloud service providers may delete the data which has rarely accessed or not has been accessed to save the storage space. In addition to that the data are lost or corrupted due to hardware errors and software bugs. Thus the main obstacle is integrity of outsourced files. So the security of the outsourced data must be ensured. For checking the data are correctly stored in the cloud the user needs to periodically check data integrity. Thus the biggest challenge is how to perform periodical integrity checking without the local copy of data files. And it is impractical to download the whole data file to check data integrity for a data user.

To address this issue Considerable efforts have been made such as Provable Data Possession (PDP) [2] for proof of storage (PoS) and Proof of Retrievability (PoR) [3]. But some critical issues are there in the existing proposals such as first, most schemes lack a controlled way of delegatable outsourcing. The delegator can't approve regardless of whether the approved one has upload the document as determined or check regardless of whether the transferred file has been kept intact. For solving this problem Identity is provided to users in the proposed system. The key exchange between administrator and users are secured by using ECDH [20] algorithm. Second issue is data log related auditing is not included in the existing PoS-like schemes, such as PDP and Proofs of Retrievability (PoR).For solving the second issue data log related auditing is included in the proposed system. Third issue is the security of files in the cloud storage. So for solving this files are encrypted using AES[7] , [21]algorithm.

A. Related Work

Juels and Kaliski introduced PoR [3]. By using PoR regular checks of file retrievability can be done efficiently. But only a limit number of integrity queries on the outsourced files are supported in [3] because sentinels are used for detecting unauthorized modifications. The first three PoR schemes with strict security proofs are introduced by Shacham and Waters [9]. It supports private and public verifiability. For strengthens the security and availability of outsourced files in the standard PoR framework Bowers *et al.* [27] introduced PoR in multi-server setting. Armknecht *et al.* [22] examined delegatable auditing for privately auditable PoR schemes and introduced a new scheme in which it simultaneously protects the files from collusion attacks by auditors, cloud servers and malicious clients.

The thought of PDP presented by Ateniese et al. [2] without retrieving the entire file from the cloud server it enables an auditor to check the integrity of an outsourced file, at the same time for answering integrity queries the server does not need to access the entire file. A subsequent work in [4] the outsourced data can be deleted modified but insertion operation is not possible. Yang and Jia in [26] introduced a scheme in which dynamic update for the outsourced data is supported. Wang *et al.* [16] introduced new scheme in which he include a third security-mediator into PDP system. The security-mediator learns nothing about the file he generate verifiable metadata on the outsourced files in a blind way. For supporting data migration Zhu *et al.* [12] introduced a cooperative PDP scheme.

Wang *et al.* [10] proposed a cloud storage scheme using proxy re-signatures. It is a secure cloud storage scheme because if some user is revoked, then her outsourced data will be re-signed by the cloud storage server. For supporting multicloud storage scenario Wang [28] introduced a secure identity-based scheme. Identity-based PDP scheme is introduced in [29]. It support group oriented applications. Yu *et al.* [11] introduced new scheme for solving key-exposure problem in secure cloud storage. Chen *et al.* [30] find the relationship between secure networking coding and secure cloud storage and introduced a new scheme in which a systematic way is presented to construct a secure cloud storage scheme from any secure networking coding protocol.

Without leaking the private information of data owner he can delegate the rights of integrity auditing to a third party auditor (TPA) for this Public verifiability property is used. By using this property any person can audit the outsourced data without knowing the private parameters of the data owner. The schemes in [2], [10], [30], [4], [16], [12], [28] are all publicly verifiable. Using the vector commitment technique Jiang et al. [14] recently introduced a publicly verifiable scheme. It also supports secure user revocation. Against the auditor in auditing integrity Yu et al. [28], Yu et al.[27] and Fan et al. [15] considered in distinguishability/ privacy on outsourced data. Zhang and Dong's publicly verifiable data outsourcing scheme [29] is proved with tight security reduction in ID-based setting. A certificateless public verification scheme is introduced by Zhang et al. [17].It provides stronger security against a malicious auditor.

For supporting delegatable integrity auditing on outsourced files some schemes are introduced but they cannot support control delegatable outsourcing. In privacy-preserving public auditing cloud storage schemes presented by Wang *et al.* [25], a secure TPA is there for verifying the integrity of outsourced files, while TPA can't access the file's content. Wang in [23] introduced a proxy PDP scheme in which the authorized proxy can be delegated for conducting data possession checking if the designated auditor is

unavailable. Wang *et al.* [13] proposed a secure data outsourcing scheme in the identity-based setting, it is a variant of the Schnorr signature. But this scheme does not support delegated data outsourcing mechanism. Yujue Wang in [1] supports delegatable identity based data outsourcing but the key exchange between the registry server and users is not secure.

B. Paper Organization

We describe the system architecture, system model and security goals in Section II. The methodology of the system in Section III. The security and performance of our system and the experiment and its result are analyzed in Section IV. Finally, Section V concludes the paper.

II. SYSTEM MODEL

A. System Architecture

The architecture of the proposed system is shown in Figure 1. The proposed system consists of four types of entities, that is, admin/file-owners, proxies, auditors, and server. Generally, the admin/file-owners, proxies and auditors are cloud clients. The admin/file-owner is the administrator of the system responsible for setting up the system and he is also responsible for registering the proxies and auditor and he can also upload files to the server. The server provides storage services to the registered clients for storing outsourced files. In real-world applications, an organization buys storage services from some CSP. In this way, the registered clients (employees) can take advantage of the storage services.

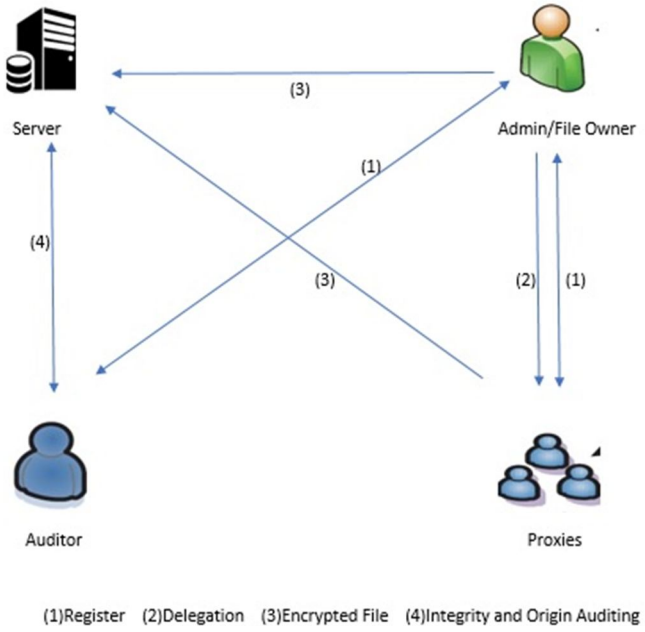


Figure 1: The architecture of the system

The authorized proxies and admin/file-owner can outsource files to the cloud server. A lot of files are there in an organization, it's difficult to upload all these files by admin/file-owner. By this system on behalf of the owner, the authorized proxy encrypt the file, sends the encrypted file to the server. Neither the proxy nor the file-owner is required to store the original file or the encrypted file locally. The file can be retrieved at any time from the server when required. Checking the integrity of outsourced files and their origin-like general log information is the duty of the auditor. Without retrieving the entire file the integrity of the outsourced file can be checked by interacting with the server.

B. Adversary Model and Security Goals

The proposed system confronts two types of active attacks. The first one is for saving storage space a malicious storage server may modify or even remove the outsourced files, especially for the rarely accessed files, or due to hardware failures the files may be lost. Second, the cloud client may impersonate others, that means he may impersonate an authorized proxy or owner, or abuse a delegation, and in this way he can process a file and outsource it to the storage server in an unwanted way. The other problem is the files in the server may access by attackers. For preventing these attacks, a secure system should satisfy the following requirements:

1) *Dedicated delegation:* To outsource specified files in a designated way a delegation is issued by a file-owner and it can only be used by the specific authorized proxy. Even the authorized proxy cannot outsource unspecified files, the file-owner specifies the type of the file and the time is also set by the owner. The authorized proxy can upload the files based on these time and the file type.
2) *Comprehensive auditing:* Normally the integrity of the outsourced file is audited. But here the auditor verifies the log information about the type, origin and consistence of the outsourced files. For ensuring that the outsourced files have been kept intact the integrity auditing is done. For ensuring the file has been outsourced in the designated way the other general log information auditing is done.
3) *Secure key exchange:* For securing the key exchange between the admin/file-owner and the proxies ECDH algorithm is used. By using this algorithm the Key exchange can done securely and the attackers can't access the ID or passwords. For each login an OTP (One Time Password) is send to the mail ID of the users.
4) *Encryption:* The files in the server may be accessed by attackers. So for solving this problem the file must be encrypted. Here for improving the security AES algorithm is used rather than improved RSA algorithm.

III. METHODOLOGY

It is challenging to achieve both comprehensive auditing and proxy data outsourcing functionalities in IBDO. In our system this is possible. At first the admin/file-owner register proxies and auditor of the system. The admin/file-owner give the details of the proxies such as their name, mail ID, date of birth, the type of file the proxies can upload and the time period that proxies can upload files and register the proxies. The admin/file-owner can upload files. He can also view the files uploaded by the proxies.

The key exchange between the admin/file-owner and the proxies are secured by ECDH algorithm. ECDH is a variant form of DH (Diffie Hellman) algorithm. It is actually a key agreement protocol rather than a encryption algorithm. It allows two parties, each having an elliptic curve public private key pair to establish a shared secret over an insecure channel. Suppose two parties (P and Q) want to exchange key between them. The two parties generate their own private and public keys. Assume private key of P d_P and public key is $H_P = d_P G$ and private key of Q is d_Q and its public key is $H_Q = d_Q G$, P and Q use same domain parameter the same base point G on the same elliptical curve on the same finite field. P and Q then exchange public keys H_P H_Q over insecure channel. P calculates $T = d_P H_Q$ and Q calculates $T = d_Q H_P$. Like this key can be exchanged securely.

The authorized proxies can upload files based on the time allotted by the admin/file-owner and can only upload the specified type of file. The file is encrypted before uploading. AES algorithm is used for encryption. AES is based on substitution–permutation network. Using a series of linked operations AES encrypts the file. These include substitution (replacing inputs by specific outputs) and permutations (shuffling bits).Rather than bits AES performs all its computations on bytes. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. The first transformation in the AES encryption cipher is substitution of data using a substitution table. The second transformation shifts data rows. The third mix columns. The last transformation is a simple exclusive or operation performed on each column using a different part of the encryption key. Longer keys need more rounds to complete.

The proxies and admin/file-owner can delete the local copy of the file. The file is there in the server and it can be retrieved when they required. For checking the data integrity and origin auditing an auditor is there. The auditor can audit the integrity of data and he can also check the type of data each proxy loaded and also check the origin of the data.

IV. EXPERIMENTAL RESULTS

We conducted experiments on our scheme and the existing schemes. And found that our scheme is better than the existing scheme. Figure 2 shows graph time Vs file size. Blue colour in the graph shows the normal case and yellow colour indicates when proxies are used to upload files. From the graph it is clear that when using proxies less time is required to upload files.

By analyzing Table-1, for both encryption and decryption process time taken by RSA algorithm is much higher compare to the time taken by AES and DES algorithm. Variation in buffer size is noticed. It does not increase according to size of file in all algorithms.

By analyzing Figure 3, it shows buffer size usages by RSA, DES and AES algorithm and noticed that RSA algorithm buffer size usages are highest for all sizes of document file.

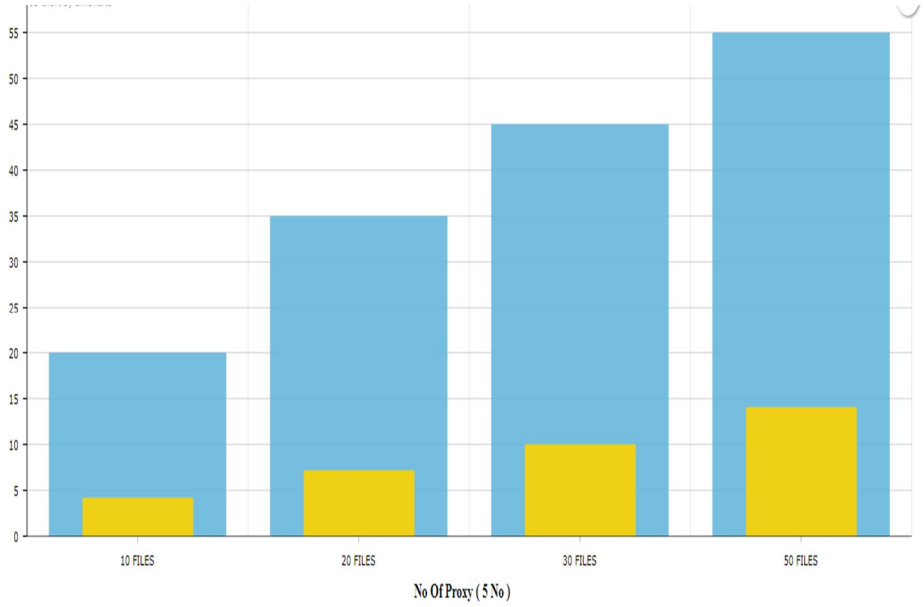


Figure 2: Time VS File size

S.NO	Algorithm	Pack Size (KB)	Encrypt Time (Sec)	Decrypt Time (Sec)	Buffer Size
1	DES	153	3.0	1	157
	AES		1.6	1.1	152
	RSA		7.3	4.9	222
2	DES	118	3.2	1.2	121
	AES		1.7	1.2	110
	RSA		10.0	5.0	188
3	DES	196	2.0	1.4	201
	AES		1.7	1.24	200
	RSA		8.5	5.9	257
4	DES	868	4.0	1.8	888
	AES		2.0	1.2	889
	RSA		8.2	5.1	934
5	DES	312	3.0	1.6	319
	AES		1.8	1.3	300
	RSA		7.8	5.1	416

Table 1: Comparison of various packet sizes for RSA
DES and AES algorithm

Figure 4 shows the comparison graph between the RSA improved RSA and AES. From this graph it is clear that AES is better than RSA and improved RSA. We examined the time taken by each algorithm for encrypting the file and also examined the time taken by each when increasing the size of the document. RSA shows poor performance compared to the other two. In the case of improved RSA it shows better performance than RSA but when the size of packet is above 310 it takes more time to execute. AES shows steady performance. When packet size increases there is only a small change in time taken.

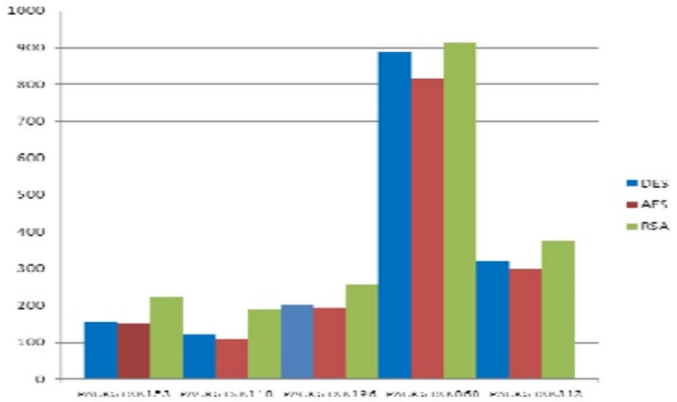


Figure 3: Comparative analysis of Buffer Size among RSA, DES and AES algorithm

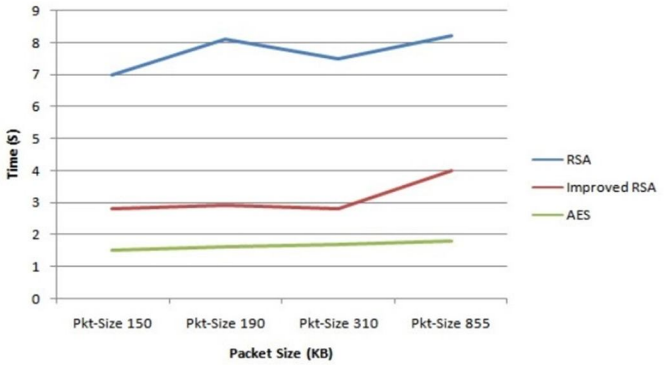


Figure 4: Comparison between RSA, improved RSA and AES

V. CONCLUSION

This paper present a new scheme which allows the file-owner to delegate his outsourcing capability to proxies. On behalf of the file-owner only the authorized proxy can process and outsource the file. Both the file integrity and file origin can be verified by an auditor. The identity based feature and the comprehensive auditing feature make the scheme advantageous over existing PDP/PoR schemes. Compared to existing PoS like proposals, this scheme has features like Identity-based outsourcing, comprehensive auditing, and strong security guarantee. Admin/file-owner and the authorized proxies can securely outsource files to a remote server which is not fully trustable, while any unauthorized ones cannot outsource files on behalf of the user. With the identities the cloud clients, including the file-owners, proxies and auditors are recognized, which avoids the usage of complicated cryptographic certificates. Even if the files might be outsourced by different clients, the integrity of outsourced files can be efficiently verified by an auditor. Also, the information about the origin, type and consistence of outsourced files can be publicly audited. The files are encrypted using AES algorithm, thus the files are secure. Experimental results show that the proposed scheme is secure and has comparable performance as the existing system.

VI. ACKNOWLEDGEMENT

This work has begun as a part of Master's Degree project. In this respect, the authors would like to thank the staffs of the college. I express my special gratitude to the HOD in charge of Computer Science and Engineering department Mr. Sarath V sankaran, for providing me constant guidance and encouragement. I express my sincere gratitude to Mr. Shyjith M B, for his inspiration and timely suggestions. Along with that lots of thanks to the authors who gave enlightenment to this survey through their papers.

REFERENCES

[1] Yujue Wang, Qianhong Wu, Bo Qin, Wenchang Shi, Robert H. Deng, and Jiankun Hu, "Identity-Based Data Outsourcing With Comprehensive Auditing in Clouds"

[2] G. Ateniese et al, "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., New York, NY,USA, , pp. 598–609, 2007.

[3] A. Juels and B. S. Kaliski, Jr, "PORs: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., New York, NY, USA, , pp. 584–597, 2007.

[4] G. Ateniese, R. di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., New York, NY, USA, Art. no.9, 2008.

[5] Y. Yu et al, "Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage," Int. J. Inf. Secur., vol. 14, no. 4, pp. 307–318, August 2015.

[6] Y. Yu et al, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," in IEEE Trans. Inf. Forensics Security, to be published, 2016.

[7] Daniyal M. Alghazzawi, Syed Hamid Hasan and Mohamed Salim Trigui "Advanced Encryption Standard - Cryptanalysis research" in Computing for Sustainable Global Development (INDIACom), 2014 International Conference on 5-7 March 2014.

[8] J. Zhang and Q. Dong, "Efficient ID-based public auditing for the outsourced data in cloud storage," Inf. Sci., vols. 343–344, pp. 1–14, May 2016.

[9] H. Shacham and B. Waters, "Compact proofs of retrievability," in J. Cryptol., vol. 26, no. 3, pp. 442–483,2013.

[10] B. Wang, B. Li, and H. Li,"Panda: Public auditing for shared data with efficient user revocation in the cloud," in IEEE Trans. Serv. Comput., vol. 8, no. 1, pp. 92–106,Februvary 2015.

[11] J. Yu, K. Ren, C. Wang, and V. Varadharajan,"Enabling cloud storage auditing with key-exposure resistance,"in IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167–1179,June 2015.

[12] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu,"Cooperative provable data possession for integrity verification in multi cloud storage," in IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231–2244, December 2012.

[13] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer,"Identity-based remote data possession checking in public clouds," Inf. Security, IET, vol. 8, no. 2, pp. 114–121,March 2014 .

[14] T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," IEEE Trans. Comput., vol. 65, no. 8, pp. 2363–2373, Aug. 2016.

[15] X. Fan, G. Yang, Y. Mu, and Y. Yu, "On indistinguishability in remote data integrity checking," Comput. J., vol. 58, no. 4, pp. 823–830, 2015.

[16] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing shared data on the cloud via security-mediator," in Proc. IEEE 33rd Int. Conf. Distrib. Comput. Syst. (ICDCS), pp. 124–133, July 2013.

[17] Y. Zhang, C. Xu, S. Yu, H. Li, and X. Zhang, "SCLPV: Secure certificateless public verification for cloud-based cyber-physical-social systems against malicious auditors," IEEE Trans. Comput. Social Syst., vol. 2, no. 4, pp. 159–170, Dec. 2015.

[18] C.K. Chu, W.T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," in IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct. 2013.

[19] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud data protection for the masses," in Computer, vol. 45, no. 1, pp. 39–45, Jan. 2012.

[20] Ruchika Markan and Gurvinder Kaur "Literature Survey on Elliptic Curve Encryption Techniques" in International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 9, Page | 906, September 2013

[21] Sandeep Kumar Rao, Dindayal Mahto and Dr. Danish Ali Khan, " A Survey on Advanced Encryption Standard", in International Journal of Science and Research (IJSR) , Volume 6 Issue 1, January 2017.

[22] F. Armknecht, J.-M. Bohli, G. O. Karame, Z. Liu, and C. A. Reuter, "Outsourced proofs of retrievability," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., New York, NY, USA, pp. 831–843, November 2014.

[23] H. Wang, "Proxy provable data possession in public clouds," in IEEE Trans. Services Comput., vol. 6, no. 4, pp. 551–559, Oct./Dec. 2013.

[24] C.K. Chu, W.T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," in IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct. 2013.

[25] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 275–362, Feb. 2013.

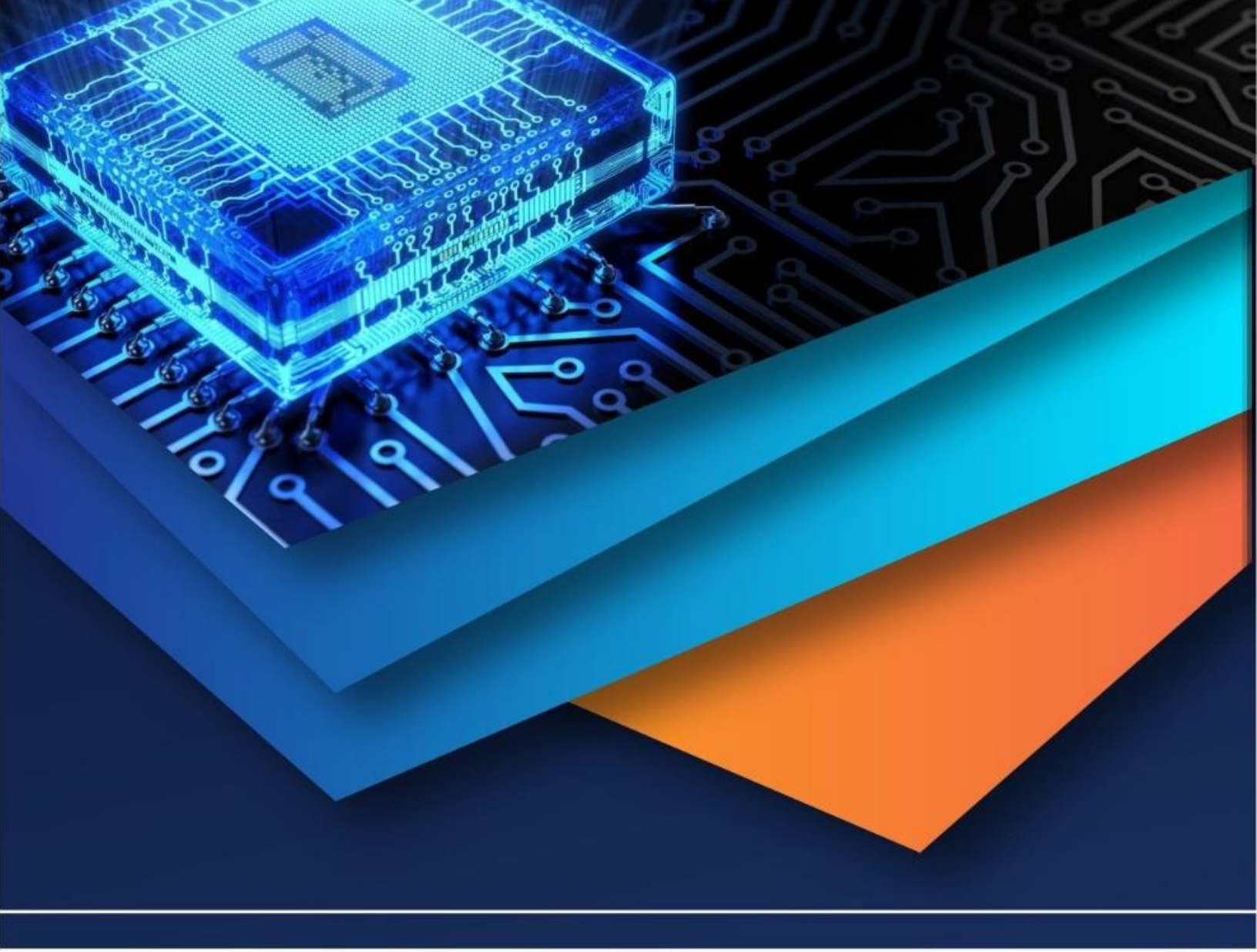
[26] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

[27] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," in Proc. 16th ACM Conf. Comput. Commun. Secur., New York, NY, USA, 2009, pp. 187–198.

[28] H. Wang, "Identity-based distributed provable data possession in multicloud storage," IEEE Trans. Services Computing, vol. 8, no. 2, pp. 328–340, Mar. 2015.

[29] Y. Wang, Q. Wu, B. Qin, X. Chen, X. Chen, X. Huang, and J. Lou, "Ownership-hidden group-oriented proofs of storage from pre-homomorphic signatures," Peer-to-Peer Netw. Appl., pp. 1–17, 2016.

[30] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, "Secure cloud storage meets with secure network coding," IEEE Trans. Comput., vol. 65, no. 6,pp. 1936–1948, Jun. 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY